FastTrace 2

FastTrace 2

by Xtralis

Technical Manual

Version 2.6 – Release 18 September 2012
Document reference 19531902

ADPRO by xtralis

General information

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Xtralis AG ("Xtralis"). You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify or publish any contents of this document without the express prior written consent of Xtralis.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, Technical and User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:

(i) in the case of services, the cost of having the services supplied again; or
(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Product Conventions

The following icons conventions are used with this product.

Convention	Description
	Caution: This icon is used to indicate that there is a danger to equipment. The danger could be loss of data, physical damage, or permanent corruption of configuration details.
	Warning: This icon is used to indicate that there is a danger of electric shock. This may lead to death or permanent injury.
	Warning: This icon is used to indicate that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

Tradename statement

ADPRO is a registered trademark of Xtralis AG Pty Ltd.

Contact Us

The Americas +1 781 740 2223
Asia +852 2916 8876
Australia and New Zealand +61 3 9936 7000
UK and Continental Europe +44 1442 242 330
The Middle East +962 6 588 5622

www.xtralis.com

Contents

General information 3
Contents 5
1 Safety instructions 11
2 Hardware 13
2.1 FastTrace 2 versus FastTrace 2 Lite 13
2.2 FastTrace 2 versus FastTrace 2☒ 14
2.3 Technical specifications 15
2.4 Hard disks 16
2.4.1 Required hard disk capacity 16
2.4.2 The ta,smart command 16
2.4.3 Add / Replace the hard disk 17
2.4.3.1 Material list (for 1 hard disk) 18
2.4.3.1.1 Mounting a second hard disk 19
2.4.3.1.1.1 With an Intel DH55TC motherboard 19
2.4.3.1.1.2 With an Intel DH61BE motherboard 21
2.4.3.1.2 Mounting a third/fourth hard disk 23
2.4.3.1.2.1 With the Intel DH55TC motherboard 23
2.4.3.1.2.2 With the Intel DH61BE motherboard 26
2.5 Fan speed selection 30
2.6 Front LED indicators 30
2.7 Required motherboard 31
2.7.1 FastTrace 2 BIOS settings 32
2.7.1.1 Motherboard Intel DG31PR or Intel DG41TY 32
2.7.1.2 Motherboard Intel DH55TC 32
2.7.1.3 Motherboard Intel DH61BE 32
2.7.2 Main & Extension I/O Cards 33
2.7.2.1 How to insert the I/O card? 33
2.7.2.1.1 Inserting the I/O cards on an Intel DG31PR motherboard 34
2.7.2.1.2 Inserting the I/O cards on an Intel DG41TY motherboard 35
2.7.2.1.3 Inserting the I/O cards on an Intel DH55TC motherboard 36
2.7.2.1.4 Inserting the I/O cards on an Intel DH61BE motherboard 37
2.7.2.1.5 Reset signal 37
2.7.2.1.6 I/O cards with mounting sets 38
2.7.2.1.6.1 Mounting order 38
2.7.3 Replacing the motherboard 38
2.8 Extension boards 39
2.8.1 Required video card 41
2.8.1.1 Replacing a video card 41
2.8.1.2 Adding a video card 41
2.8.2 DTC board 41
2.9 Available configurations 42
2.9.1 With Intel DG31PR motherboard 42
2.9.1.1 Network/monitor/keyboard 42
2.9.1.2 Extension slots 42
2.9.1.3 The Xtralis configurations 43
2.9.1.3.1 Analogue cameras (4 – 8 – 12 – 16 channels) 43
2.9.1.3.2 IP Cameras (8 or 16 channels) 43
2.9.1.3.3 Hybrid (12 channels) 43
2.9.1.3.4 Hybrid (16 channels) 43
2.9.2 With Intel DG41TY motherboard 44
2.9.2.1 Network/monitor/keyboard 44
2.9.2.2 Extension slots 44
2.9.2.3 The Xtralis configurations 45
2.9.2.3.1 Analogue cameras (4 – 8 – 12 – 16 channels) 45
2.9.2.3.2 IP Cameras (8 or 16 channels) 45
2.9.2.3.3 Hybrid (12 channels) 45
2.9.2.3.4 Hybrid (16 channels) 45
2.9.3 With Intel DH55TC motherboard 46
2.9.3.1 Network/monitor/keyboard 46

2.9.3.2 Extensions slots 46
2.9.3.3 The Xtralis configurations 47
2.9.3.3.1 Analogue cameras (4 channels) 47
2.9.3.3.2 Analogue cameras (8 channels) 47
2.9.3.3.3 Analogue cameras (12 channels) 47
2.9.3.3.4 Analogue cameras (16 channels) 47
2.9.3.3.5 IP Cameras (8 or 16 channels) 48
2.9.3.3.6 Hybrid (12 channels) 48
2.9.3.3.7 Hybrid (16 channels) 48
2.9.4 With Intel DH61BE motherboard 49
2.9.4.1 Network/monitor/keyboard 49
2.9.4.2 Extensions slots 50
2.9.4.3 The Xtralis configurations 50
2.9.4.3.1 Analogue cameras (4 channels) 50
2.9.4.3.2 Analogue cameras (8 channels) 50
2.9.4.3.3 Analogue cameras (12 channels) 51
2.9.4.3.4 Analogue cameras (16 channels) 51
2.9.4.3.5 IP Cameras (8 or 16 channels) 51
2.9.4.3.6 Hybrid (12 channels) 51
2.9.4.3.7 Hybrid (16 channels) 51
2.10 Network load 52
2.11 Current consumption 53
2.12 Maintenance 54
2.12.1 Replacing the filters 54
2.12.2 Cleaning the FastTrace 2 server 54
2.12.3 Replacing the motherboard battery 54
3 Client Setup and Configuration 55
3.1 Client software - minimum system requirements 55
3.1.1 Hardware 55
3.1.2 Software 55
3.2 Preparing your PC for installation 56
3.2.1 Internet Explorer Settings 56
3.2.2 Changing the PC's IP address 58
3.2.2.1 For Windows XP 58
3.2.2.2 For Windows 7 59
3.3 Installing the FastTrace 2 Client Software 62
3.4 Initial configuration 66
3.4.1 Launching the FastTrace 2 client in Internet Explorer 66
3.4.2 Launching the FastTrace 2 client in its own window 67
3.4.3 Adding a FastTrace 2 server to the FastTrace 2 client 69
3.4.4 Network connections 71
3.4.4.1 Ports 71
3.4.4.2 Ethernet connection 72
3.4.4.2.1 Configuring Dynamic DNS settings 73
3.4.4.2.2 Dynamic DNS error messages 73
3.4.4.2.2.1 Warning: Unable to determine IP address 73
3.4.4.2.2.2 No update required 73
3.4.4.2.3 What's the use of using Dynamic DNS? 74
3.4.4.3 Granting access to the FastTrace 2 video system 74
3.4.4.4 PPP connection 75
3.4.4.4.1 PSTN or ISDN modem Configuration 75
3.4.4.4.2 3G modem Configuration 78
4 Using IP cameras 81
4.1 Technical specifications 81
4.2 IP camera setup 82
4.2.1 General parameters 84
4.2.2 Video settings 84
4.2.2.1 Color 84
4.2.2.2 Overlay 85
4.2.3 Network 85
4.2.4 PTZ 85
4.2.5 Recording 86
4.3 Update and configure the HIPI card 87

4.4 Supported IP cameras ... 89
4.5 Video streams ... 90
5 Using analogue cameras ... 93
5.1 Technical specifications ... 93
5.2 Video & Audio Connections ... 94
5.3 Camera Configuration ... 94
5.3.1 General parameters ... 95
5.3.2 Video settings ... 95
5.3.2.1 Color ... 95
5.3.2.2 Overlay ... 96
5.3.3 Network ... 96
5.3.4 PTZ ... 97
5.3.5 Recording ... 98
5.4 PTZ settings ... 99
5.4.1 Serial PTZ ... 99
5.4.2 Serial PTZ on MIO card ... 100
5.4.3 DTC PTZ ... 101
5.4.4 List of available PTZ protocols ... 102
5.5 USB convertors ... 103
5.6 Video input termination (75 Ohm / High impedance) ... 103
6 Audio ... 105
6.1 Audio IN ... 105
6.1.1 Recommended microphones ... 105
6.1.1.1 Crown all-weather PZM-11LLWR ... 105
6.1.1.1.1 Specifications ... 105
6.1.1.1.2 Wiring diagram ... 106
6.1.1.2 ADPRO microphones IMUSTD; IMUPIR; IMUTEMP ... 106
6.1.1.2.1 Specifications ... 106
6.1.1.2.2 Wiring diagram ... 106
6.1.1.3 ADPRO Audio Unit ... 107
6.1.1.3.1 Wiring diagram ... 107
6.2 Audio OUT ... 108
6.2.1 Connecting the VM22A audio switch to the FastTrace 2 video system ... 110
7 I/O Cards Configuration ... 111
7.1 Internal I/O Cards ... 111
7.1.1 Update Main I/O card ... 113
7.1.2 USB I/O address range ... 114
7.2 Net I/O modules ... 116
7.2.1 Net I/O address range ... 117
7.2.2 Adding Net I/O module with known IP address ... 118
7.2.3 Searching Net I/O modules on the local network ... 119
7.2.4 Modifying the IP settings of a Net I/O module ... 120
7.2.5 Net I/O module inputs & outputs setup ... 121
8 Alarms ... 123
8.1 Alarm transmission ... 123
8.1.1 Default settings ... 124
8.1.2 Primary alarm transmission settings ... 125
8.1.3 Secondary alarm transmission settings ... 126
8.2 Arming/Disarming the video system ... 127
8.2.1 Arm/Disarm schedule ... 128
8.2.2 Arm/Disarm Switch ... 129
8.3 Alarm inputs ... 130
8.3.1 PTZ via I/O ... 133
8.3.2 Connecting fire detectors ... 134
8.3.2.1 Fire reset input and output ... 135
8.3.3 IntrusionTrace alarms ... 136
8.4 Alarm profiles ... 137
8.4.1 The default profiles ... 137
8.4.1.1 Normal event profile ... 138
8.4.1.2 Primary event profile ... 139
8.4.1.3 Backup event profile ... 140
8.4.1.4 Silent message profile ... 141

8.4.1.5 Single event profile ... 142
8.4.1.6 Active sensor event profile ... 143
8.4.1.7 Fire1 event profile ... 145
8.4.1.8 Fire2 event profile ... 146
8.4.1.9 Non-fire alarm profile ... 147
8.4.1.10 Fire action profile ... 148
8.4.1.11 Fire alert profile ... 149
8.4.1.12 Fire trouble profile ... 150
8.4.2 Adding a new profile ... 151
8.5 Email server settings ... 153
8.5.1 Email address book ... 153
9 Activate outputs ... 155
9.1 Manual operation ... 156
9.2 Recording controlled ... 156
9.3 Programmable output ... 157
10 Video Interconnection ... 159
11 PIR settings ... 163
11.1 Required PIR firmware ... 163
11.2 Connecting the PIRs ... 163
11.2.1 Connecting the PIR detector directly to the FastTrace 2 server (Main I/O card) ... 164
11.2.2 Connecting the PIR detector to the FastTrace 2 server using the USB to RS485 8 channel distribution unit ... 165
11.2.3 Connecting the PIR detector to the FastTrace 2 server using a USB to serial port RS485 converter ... 167
11.3 Configuring the software setting ... 168
11.3.1 Configuring the serial port ... 168
11.3.2 Initiate the PIR discovery ... 169
11.3.2.1 General ... 170
11.3.2.2 Discovery and status of the PIR detectors ... 170
11.3.2.3 Double knock configuration ... 170
12 Configuration ... 171
12.1 Storing a configuration ... 171
12.2 Activating a configuration ... 172
13 Configuring analytics ... 173
13.1 FastTrace™ 2 IntrusionTrace ... 173
13.1.1 About the FastTrace 2 Perimeter Detection analytic ... 173
13.1.2 Scope ... 174
13.1.2.1 Suitable scenes ... 174
13.1.2.2 Unsuitable scenes ... 175
13.1.3 Camera ... 176
13.1.3.1 Resolution and frame rate ... 176
13.1.3.2 Field of view (FOV) ... 176
13.1.3.3 Position ... 176
13.1.4 Configuration ... 177
13.1.4.1 Perimeter configuration interface ... 177
13.1.4.2 Cameras section ... 177
13.1.4.3 Drawing Tools section ... 178
13.1.4.4 Select IntrusionTrace license section ... 178
13.1.4.5 Info section ... 179
13.1.4.6 Advanced parameters profile section ... 179
13.1.4.6.1 Profile details ... 180
13.1.4.6.2 Tips for advanced parameters setting ... 188
13.1.4.6.3 Adding a new detection profile ... 188
13.1.4.7 Save button ... 188
13.1.5 Calibration ... 189
13.1.6 Mask zones ... 190
13.1.7 Detection zones ... 191
13.1.8 Trigger lines ... 192
13.1.8.1 Some examples ... 193
13.2 FastTrace™ 2 LoiterTrace ... 195
13.2.1 About the FastTrace 2 LoiterTrace (Loitering Detection analytic) ... 195
13.2.2 Scope ... 195
13.2.3 Camera ... 196

13.2.3.1 Resolution and frame rate ... 196
13.2.3.2 Field of View (FOV) ... 196
13.2.3.3 Position ... 196
13.2.3.4 Scene illumination ... 197
13.2.3.5 Automatic camera adaption ... 197
13.2.4 Configuration ... 198
13.2.4.1 Loitering configuration interface ... 198
13.2.4.2 Cameras section ... 198
13.2.4.3 Drawing Tools section ... 199
13.2.4.4 Select LoiterTrace license ... 199
13.2.4.5 Loitering parameters ... 200
13.2.4.6 Info section ... 200
13.2.4.7 Save button ... 200
13.2.5 Mask zones ... 201
13.2.6 Detection zones ... 202
13.2.6.1 Samples ... 203
13.3 Motion & Sabotage ... 206
13.3.1 Motion Detection Interface ... 206
13.3.2 Private zones ... 206
13.3.3 Sabotage detection ... 208
13.3.4 Motion detection ... 209
14 Active connections ... 211
15 Log ... 213
15.1 Example of a Log record ... 215
15.2 Example of an Event record ... 215
15.3 Example of a Command record ... 216
16 Presidium High Level Interface ... 217
17 Firmware, license, configuration ... 219
17.1 License types ... 220
17.2 System license ... 222
17.3 Application license ... 223
17.3.1 IntrusionTrace ... 224
17.3.2 LoiterTrace ... 224
17.3.3 Fire-IO ... 224
17.3.4 PIR-HLI ... 224
17.4 Checking the software version ... 225
17.4.1 Upgrade the Client version to the Server version ... 225
17.4.2 Downloading the new client software version from the Xtralis Support website. ... 225
17.5 Installation of the FastTrace 2 firmware ... 226
17.5.1 Installation requirements ... 226
17.5.2 Installation procedure ... 226
17.6 Upgrade the FastTrace 2 firmware ... 228
17.6.1 Upgrade requirements ... 228
17.6.2 Downloading a new firmware version from the Xtralis Support website. ... 228
17.6.3 Upgrade procedure ... 229
17.6.3.1 Upgrade firmware with BIN file ... 229
17.6.3.2 Upgrade firmware with img file ... 232
17.6.4 IP camera definitions ... 233
18 Additional information ... 235
18.1 Retrieving the IP address of the FastTrace 2 ... 235
18.2 Diagnostics ... 236
18.2.1 Retrieve traces ... 236
18.2.2 Retrieve reports ... 239
18.2.3 VSKWin: retrieve the FastTrace 2 configuration file ... 240
18.2.4 VSKWin: Create an alarm text that automatically opens a live camera image ... 241
18.2.5 Activate timer output on FastTrace 2 ... 241
18.3 Error codes ... 242
18.3.1 General error codes ... 242
18.3.2 Control protocol error codes ... 243
18.3.3 Filter graph/codec error codes ... 244
18.4 FastTrace 2 web pages ... 246
19 Labelling of products ... 247

19.1 Product number structure 248
19.2 Declaration of Conformity 249

1 Safety instructions

CAUTION

RISK OF ELECTRIC SHOCK, DO NOT OPEN!

CAUTION: TO REDUCE THE RISK OF ELECTRICAL SHOCK, DO NOT REMOVE COVERS. NO USER SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

WARNING: TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS APPLIANCE TO RAIN OR MOISTURE.

The lightning flash with an arrowhead symbol within an equilateral triangle is intended to alert the user to the presence of non-insulated “dangerous voltage” within the product’s enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

The exclamation mark within an equilateral triangle is intended to alert the user to presence of important operating and maintenance (servicing) instructions in the literature accompanying this appliance.

Environmental information	
	The crossed-out container indicates the fact that within the European Union this product has to be offered for separate waste collection at the end of the product’s lifespan. This goes for the product, but also for all accessories that are included and bear the same label. Do not put these products with domestic garbage. For more information about the ways to collect, reuse en recycle, please contact your local Waste Service. You can also contact Xtralis for more information about the environmental aspects of our products.

Clarification

ADPRO’s **FastTrace 2** is the newest ADPRO product concerning video recording. Hence, FastTrace 2 is also compatible with:

- FastTrace
- V3100
- V3100 FT
- V3100 HYBRID

You can upgrade firmware and software of the products mentioned above to the newest FastTrace 2 firmware and software. Please do take into consideration that the FastTrace 2 video system could have other system requirements than any other previous ADPRO products!

2 Hardware

2.1 FastTrace 2 versus FastTrace 2 Lite

The FastTrace 2 Lite has been designed, developed and manufactured as a complete FastTrace 2 video security system, but the ENTRY system license that is included, limits the number of cameras that can be supported to a maximum of 4 analogue cameras.

Please also note that the FastTrace 2 Lite can only operate on analogue cameras, there is no possibility to support IP cameras.

The FastTrace 2 Lite can only be purchased with an entry system license:

	FastTrace 2	FastTrace 2 Lite
Full system license	✓	✗
TX (transmission) only license	✓	✗
Entry level license	✓	✓

See System license for further information on the system licenses.

Please consult the ADPRO commercial data sheet on the FastTrace 2 Lite. This data sheet can be downloaded from our website www.xtralissecurity.com. You don't need to login to download the commercial data sheets!

2.2 FastTrace 2 versus FastTrace 2☒

The FastTrace 2☒ is the newest hardware in the ADPRO® FastTrace™ series. It has been developed as a more powerful video system with higher performance and more efficient operation.

The most important difference is the possibility to have **16 analytic channels** with the FastTrace 2☒, while the FastTrace 2 is limited to a maximum of 4 analytic streams.

The FastTrace 2☒ can also be purchased with a full or tx only system license:

	FastTrace 2	FastTrace 2☒
Full system license	✓	✓
TX (transmission) only license	✓	✓
Entry level license	✓	✗

See System license for further information on the system licenses.

Mind:

The FastTrace 2☒ requires the minimal software version 2.6!

Please note:

Wherever in this document the term FastTrace 2 is used, you can assume that the term refers to both the FastTrace 2 and the FastTrace 2☒, unless specifically mentioned otherwise!

2.3 Technical specifications

Operating system	PC platform – Linux OS
Network protocols	TCP, UDP, FTP, TELNET, HTTP, SMTP, RTSP, RTP
Bandwidth	Remotely adjustable: compression, fps and quality. A bandwidth limit can be specified.
Bandwidth consumption	6 fps CIF/SIF: 70 kb/sec 12 fps 4CIF/SIF: 400 kb/sec in optimal quality
Software updates	Local and remote
Maximum number of cameras	16 (total of analogue and IP cameras)
Web server	Integrated
COM ports	4 USB interfaces used for: - PTZ control (requires USB ➞ RS485 convertor) - PSTN or ISDN modem
Ethernet	10/100/1000 Base-T, auto detection, full duplex, RJ45
Storage	up to 4 devices (connected through SATA interfaces); following arrangements are possible: - 1 to 4 hard disks (500 GB to 2 TB) **Remark:** There are USB connectors accessible on the back of the FastTrace 2 video system; and also 1 USB connector is on the front to which a portable DVD writer can be connected to export video sequences.
Remote visualisation	Internet Explorer; Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008
Management	- Internet Explorer (installs Client software) - VSKwin software - M3000 software - VideoCentral Platinum - 3rd party CMS software
Power supply	100~240 VAC, 50/60 Hz (+80% efficiency) **! The video system has to be connected to a 230 VAC/16A mains outlet with proper earth, applying a separate locally approved power cord.**
Operating temperature	5 – 40°C (*see also Fan speed selection*)
Humidity	20 – 93% (non condensing)
Dimensions	445x132,50x300 (WxHxD in mm) *Rubber feet can be fixed on the bottom. The height is then increased with 2.5 mm.*

Multi-site FASTTRACE 2 configuration is possible:
- Integration of up to 10,000 FastTrace 2 video security systems.
- Remote video and audio, live video and consultation of recordings.
- Compatible with FOXnet®Plus, FALCONnet, S3100, Presidium, VSKwin®, VCP and M3000.
- SDK for third party integration.

2.4 Hard disks

2.4.1 Required hard disk capacity

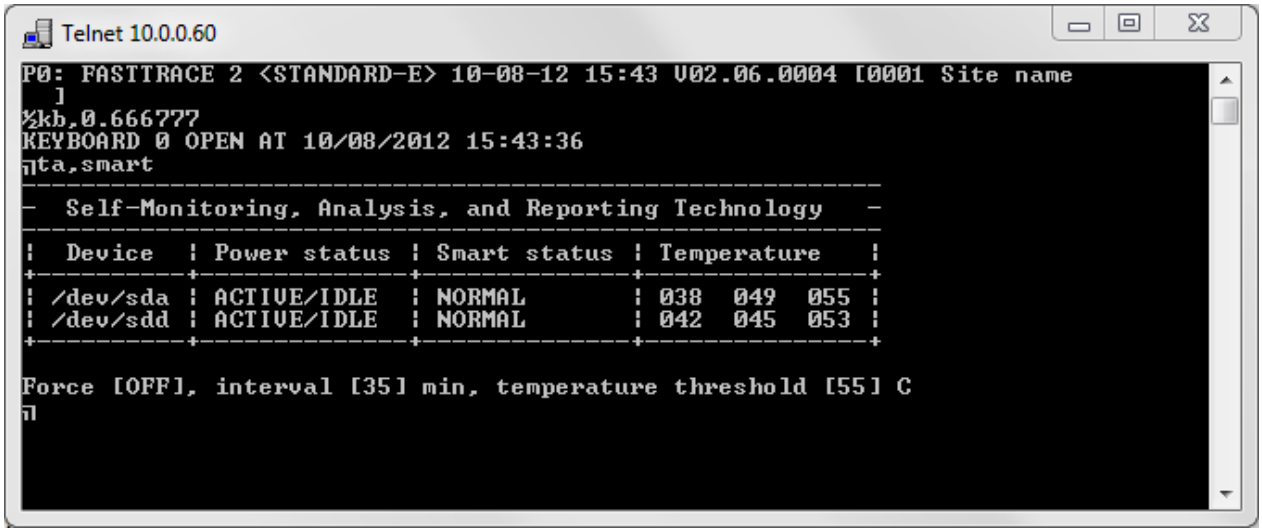
As there are lots of configuration possibilities, a *hard disk space calculator* has been made available. You can find this *hard disk space calculator* on the CD/DVD provided with your FastTrace 2 video system, or you can download it from our website http://www.xtralissecurity.com. Make sure you log in with sufficient download rights!

Mind:

The calculator is an estimating tool only. Figures are purely indicative. The real results of the hard disk capacity depend on scene content.

2.4.2 The ta,smart command

SMART stands for Self-Monitoring Analysis and Reporting Technology. When executing the **ta,smart** command in a TELNET session, you will become the SMART information for all hard disks in the video system FastTrace 2.

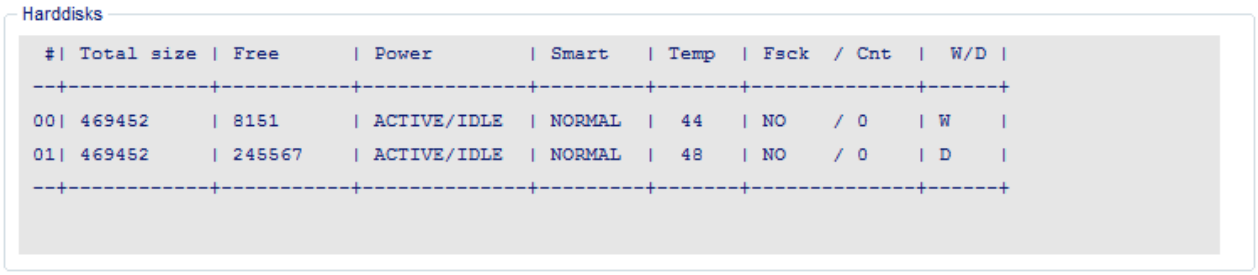

Telnet 10.0.0.60
P0: FASTTRACE 2 <STANDARD-E> 10-08-12 15:43 V02.06.0004 [0001 Site name
]
½kb,0.666777
KEYBOARD 0 OPEN AT 10/08/2012 15:43:36
ta,smart
Self-Monitoring, Analysis, and Reporting Technology
Device | Power status | Smart status | Temperature
/dev/sda | ACTIVE/IDLE | NORMAL | 038 049 055
/dev/sdd | ACTIVE/IDLE | NORMAL | 042 045 053
Force [OFF], interval [35] min, temperature threshold [55] C

Device	Indicates the specific hard disk
Power status	The power status column can display 1 of these statuses: > ERROR ➞ problem retrieving power status of the drive > ACTIVE/IDLE ➞ normal operation of the drive > STANDBY ➞ drive is in low power mode (drive has spun down) > SLEEPING ➞ drive is in lowest power mode (drive is completely shut down)
Smart status	The smart status column can display 1 of these statutes: > ERROR ➞ drive is failing > ALERT ➞ there's a problem retrieving smart info from the drive or the drive could start having trouble > NORMAL ➞ no problems found with the drive
Temperature	The temperature column display from left to right: > the minimum temperature of the disk > the current temperature of the disk > the maximum temperature of the disk

Force [ON/OFF]	ON = smart is checked on disk in STANDBY or SLEEPING mode; OFF = smart is only checked on disks in ACTIVE/IDLE mode
Interval	Indicates the interval time between smart checks. The value is expressed in minutes.
Temperature threshold	if disk temp is higher than this threshold, an alarm is generated: I102: 'SMART HDD ALERT TEMP'

2.4.3 Add / Replace the hard disk

When you receive an error message from your hard disk in the *Status* window of the FastTrace 2 Client, you might need to replace the faulty hard disk. If you have 2 or more hard disks installed in your FastTrace 2 server, you can check which hard disk is causing the alarm messages in the FastTrace 2 Client via **System > Maintenance > Harddisks**. In the column *Smart* you will get the operational status of the hard disks. You can also retrieve this information via the Telnet command **ta,smart** (see The ta,smart command).


Harddisks
#| Total size | Free | Power | Smart | Temp | Fsck / Cnt | W/D |
00| 469452 | 8151 | ACTIVE/IDLE | NORMAL | 44 | NO / 0 | W |
01| 469452 | 245567 | ACTIVE/IDLE | NORMAL | 48 | NO / 0 | D

Switch off power supply and replace the hard disk. You can also add a new hard disk without removing any of the hard disks in use. Up to 4 hard disks can be installed.

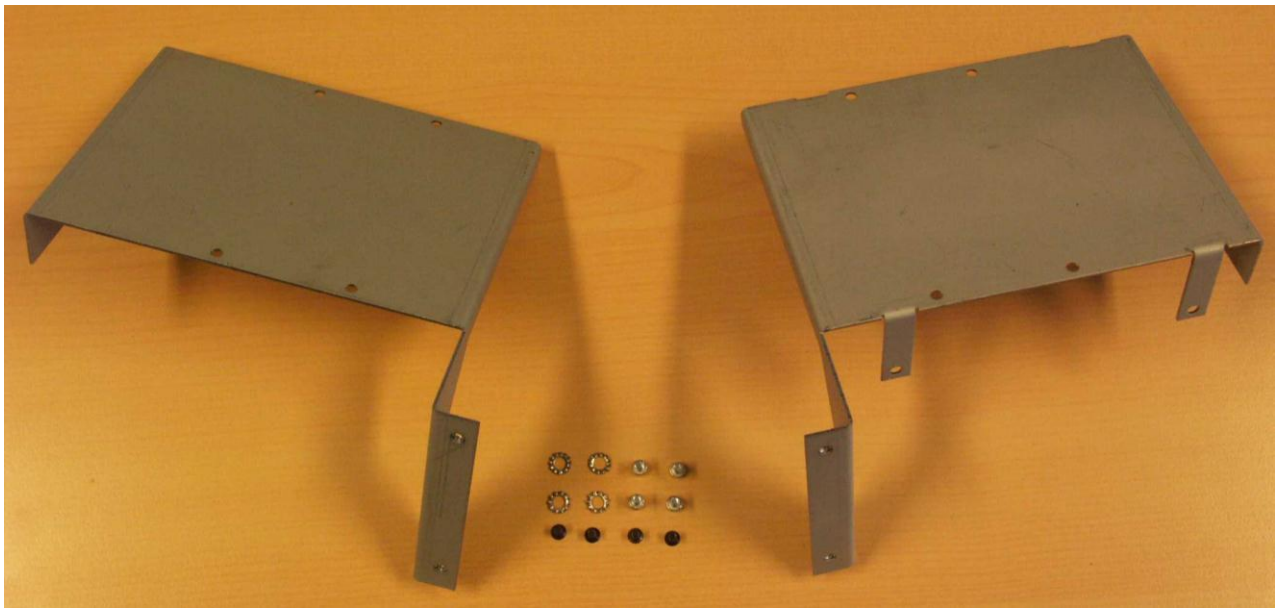
Important:

It is possible to mount a hard disk coming from another unit into the installer. Thus you can playback video recordings that have been recorded by another FastTrace 2 unit.

Some restrictions need to be taken into account though:

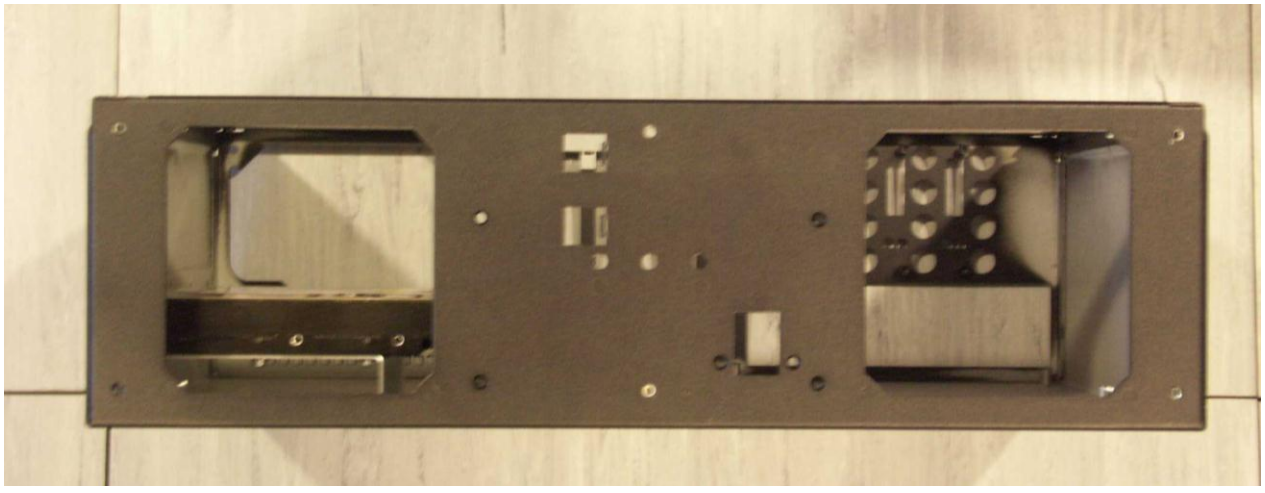
- It is advised to immediately put the number of days recording to 0, thus preventing overwriting of valuable data.
- Clear all recording conditions in the recording behaviour, thus preventing overwriting of valuable data.
- Do not mix hard disks from different FastTrace 2 units into one, because this will result in unpredictable behaviour.

2.4.3.1 Material list (for 1 hard disk)



Part	Amount + reference number
Support for disk 2	1x #17291210
Support for disk 3 and 4	1x #17291220
Disk screws	4x #17434080 or #17434060
Dented washers M4	4x #17720050
Mounting screws	4x #17439080
Sata cable	1x #16520870 (for DH55TC motherboard) 1x #16520875 (for DH61BE motherboard)

Remove the lid. Then remove the front plate. You can now see the mounting holes for the disk bays.



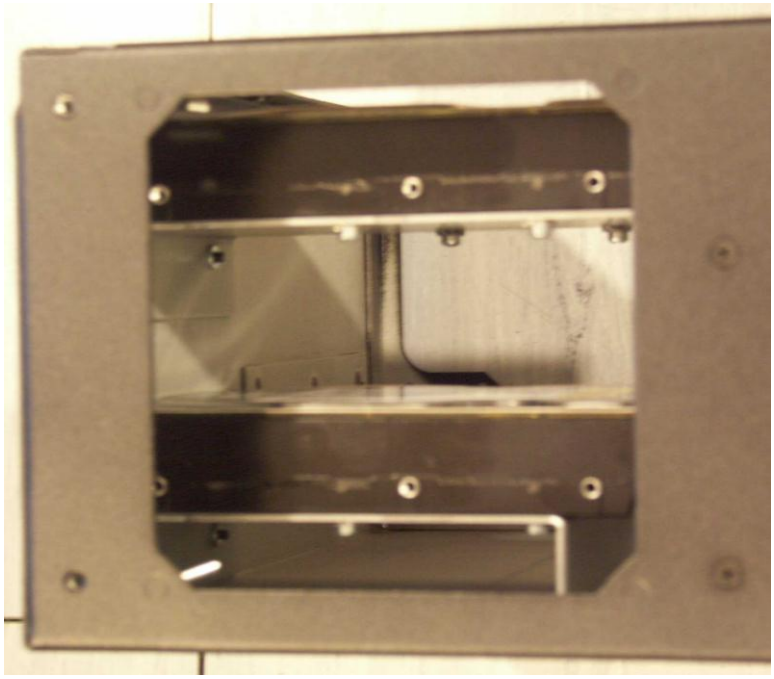
Install the internal disk(s) into the supports with screws # 17434080 or # 17434060 and dented washers M4 # 17720050.

2.4.3.1.1 Mounting a second hard disk

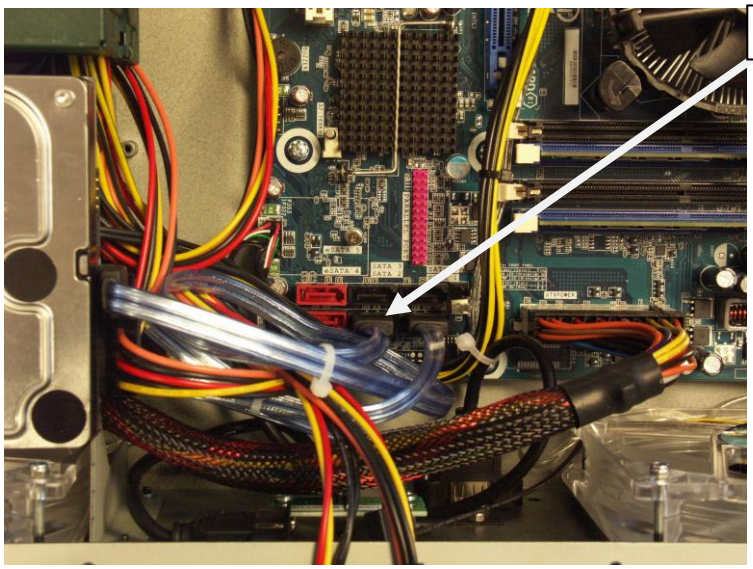
2.4.3.1.1.1 With an Intel DH55TC motherboard

Fix the second disk onto the support at the power supply side.

Next, install the support with the screws (# 17439080) at the front and on the left side of the casing.



Then connect to eSATA2 with the SATA cable (# 16520870).

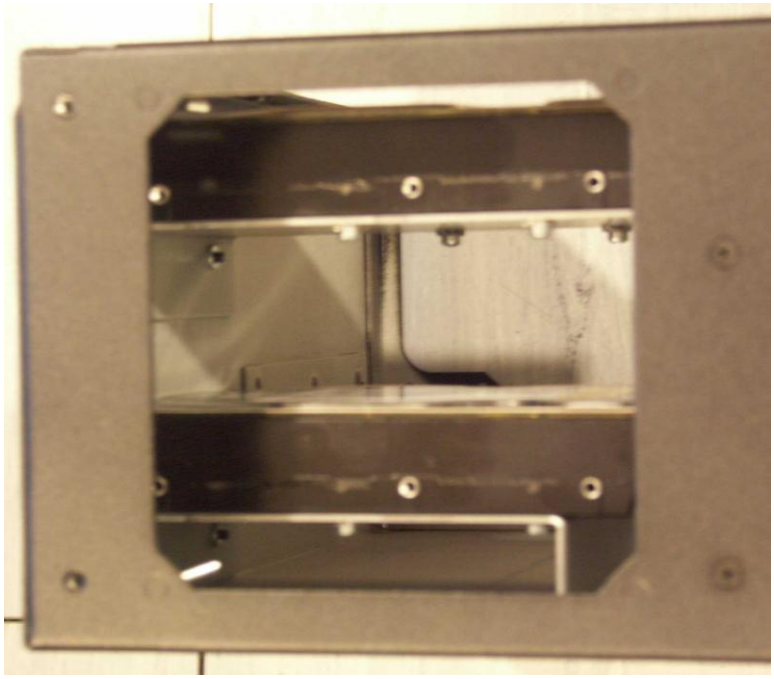


Attention:
Connect the remaining SATA power connector (not the one on the tail end from the disk 1 cable) onto the disk.

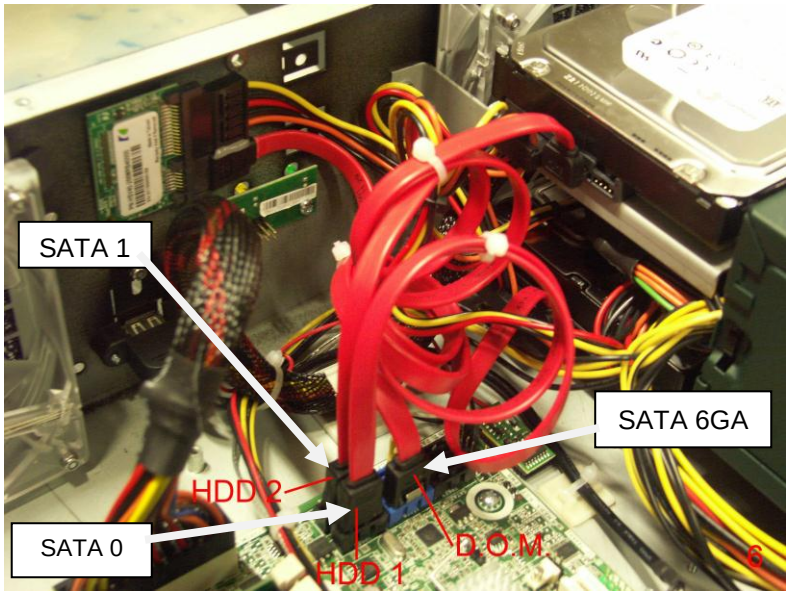
2.4.3.1.1.2 With an Intel DH61BE motherboard

Fix the second disk onto the support at the power supply side.

Next, install the support with the screws (# 17439080) at the front and on the left side of the casing.



Then connect to SATA1 with the SATA cable (# 16520875).

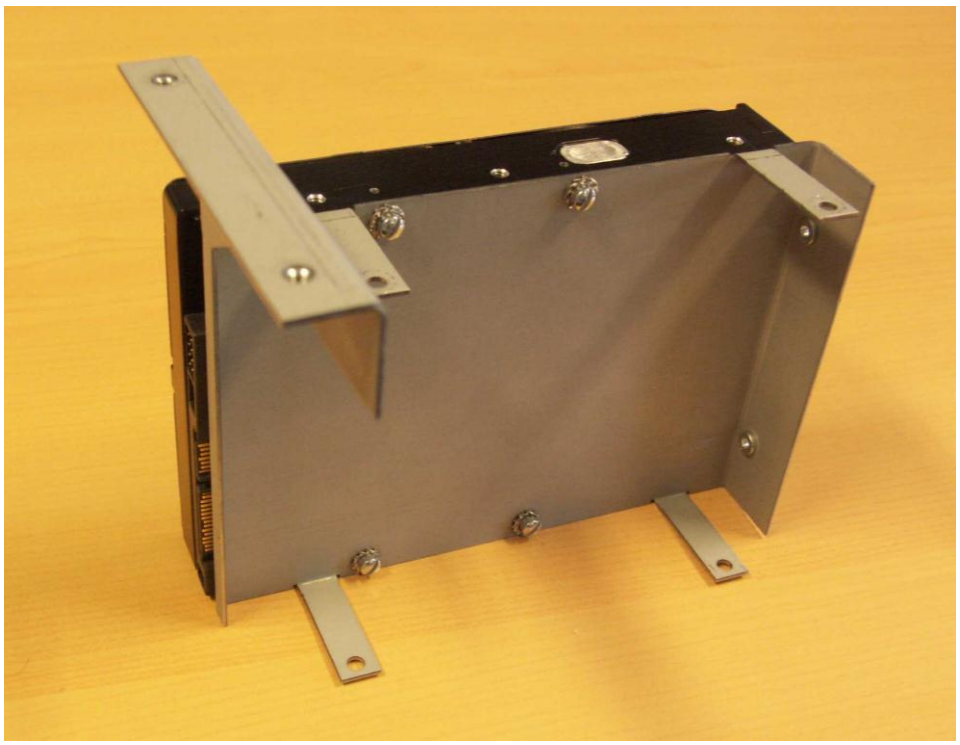


Attention:
Connect the remaining SATA power connector (not the one on the tail end from the disk 1 cable) onto the disk.

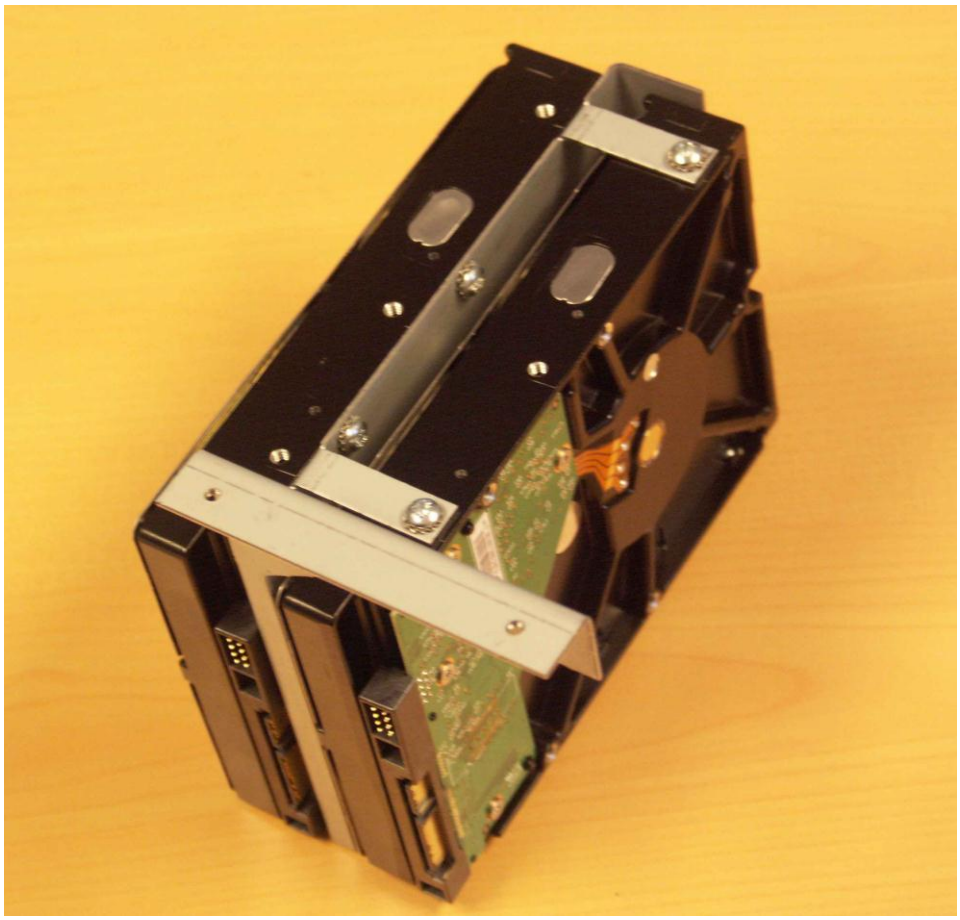
2.4.3.1.2 Mounting a third/fourth hard disk

2.4.3.1.2.1 With the Intel DH55TC motherboard

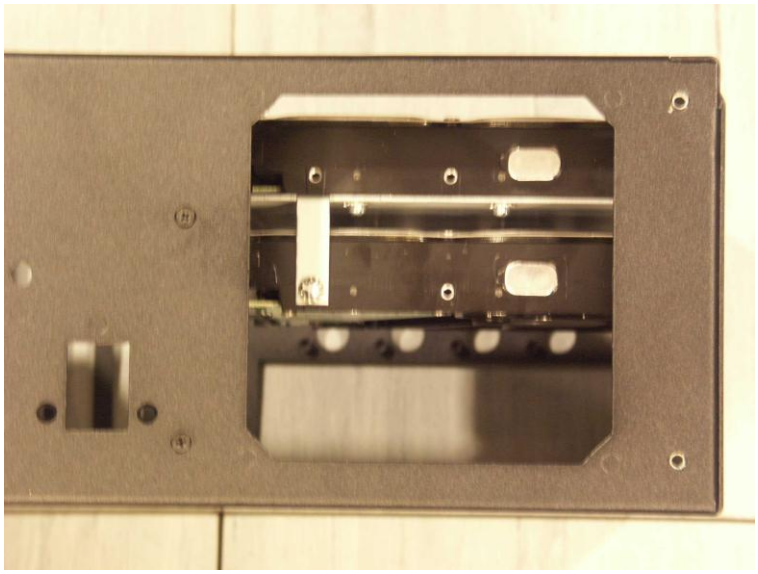
Fix the third disk on the topside of the third support (mount before the fourth).



Fix – if desired – the fourth disk on the bottom side of the same support.

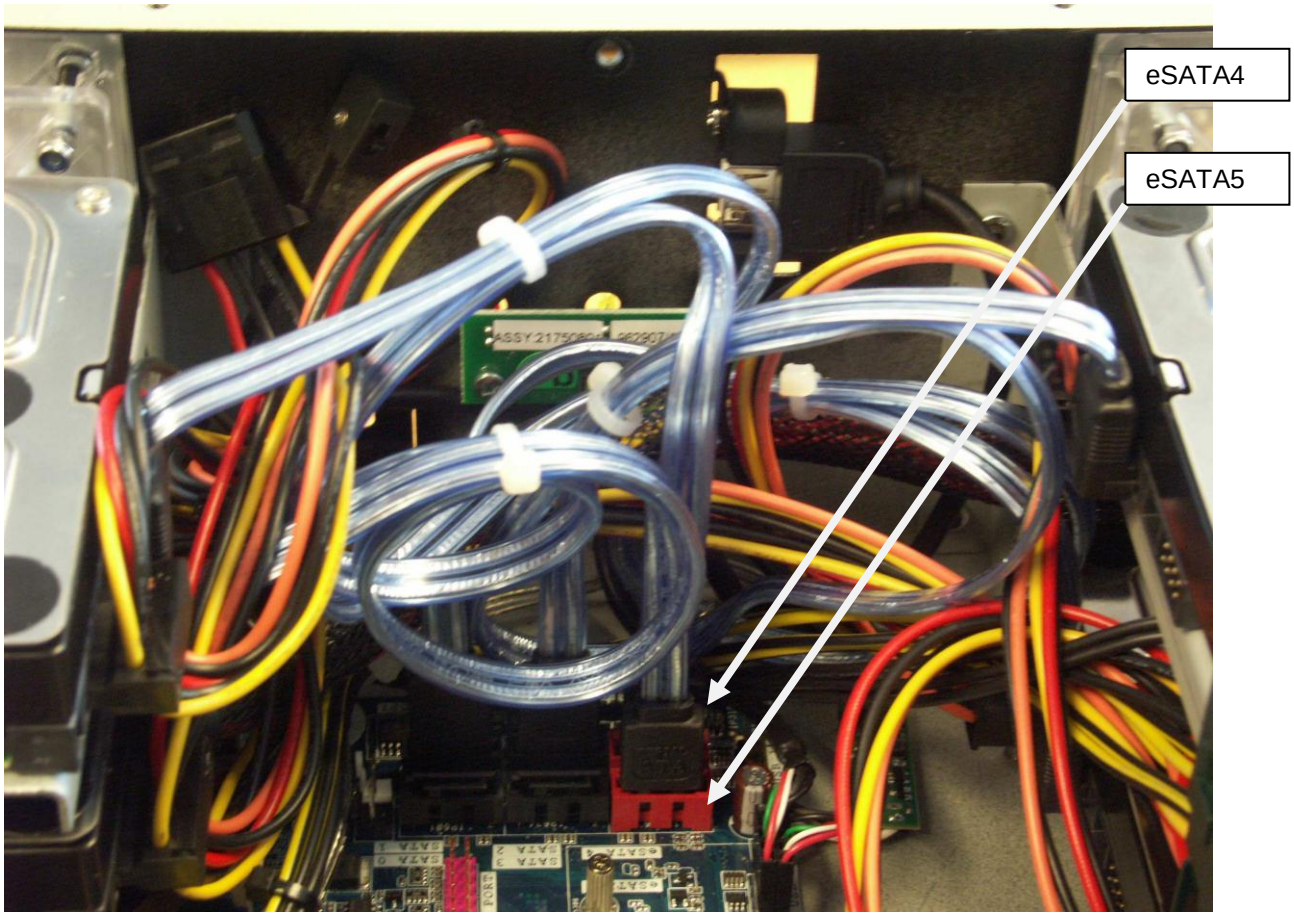


Install the support with two screws (# 17439080) at the front and on the right side of the casing.



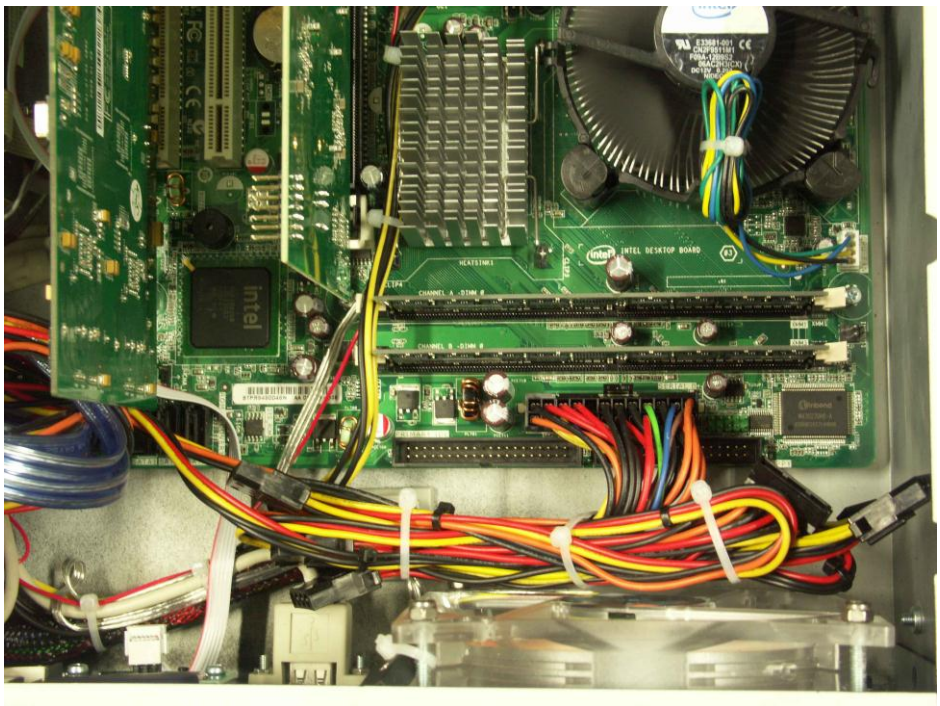
Then connect disk 3 to eSATA4 connector with the SATA cable (# 16520870).

When disk 4 is in use connect it to eSATA5 connector with the SATA cable (# 16520870).



Pay attention: Do not bend the SATA cables too sharp to avoid cable damage!

Use tie-wraps to bundle the unused SATA power cables.



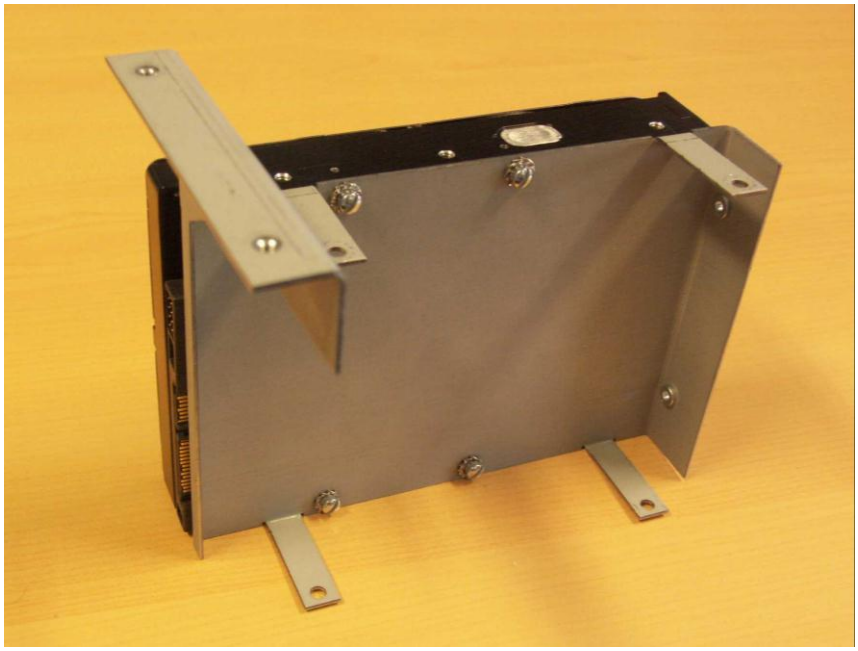
Then fix the front plate (# 17011610) on the base with the screws (# 17444080).
Put the cover in place and secure with 10 screws (# 17439080).

Connect monitor/screen and keyboard to the FastTrace 2 Server. Switch on power supply and wait for the boot window. Select **<FastTrace 2 Installer>** during startup. Next, select **Update current system > Manage recording disks** and select the new hard disk from the list. Press 'Enter'. Then select – use the TAB button – "**Format and use selected disk**". Select **Main Menu** and choose **Reboot**.

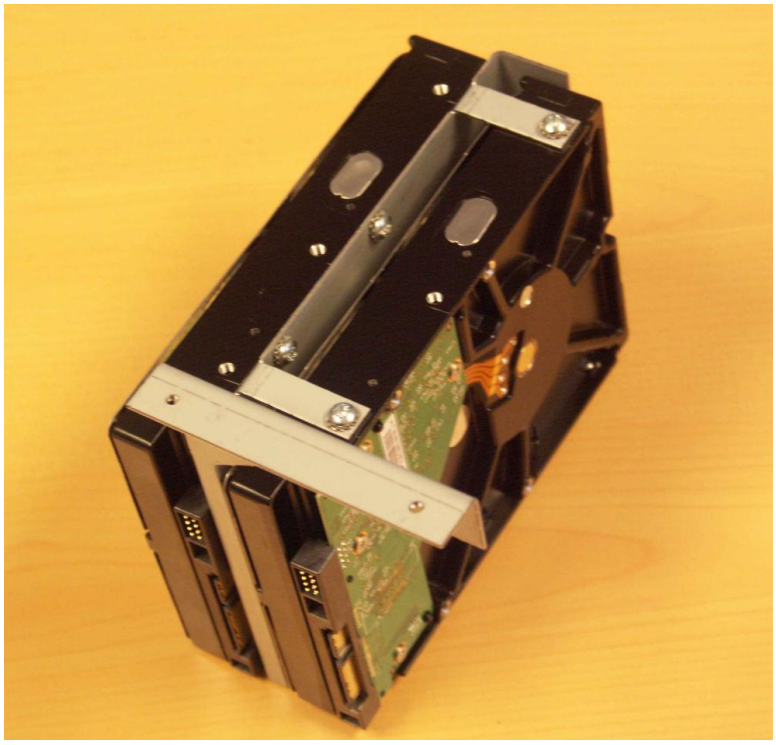
The video system will now reboot. After rebooting the new hard disk can be used.

2.4.3.1.2.2 With the Intel DH61BE motherboard

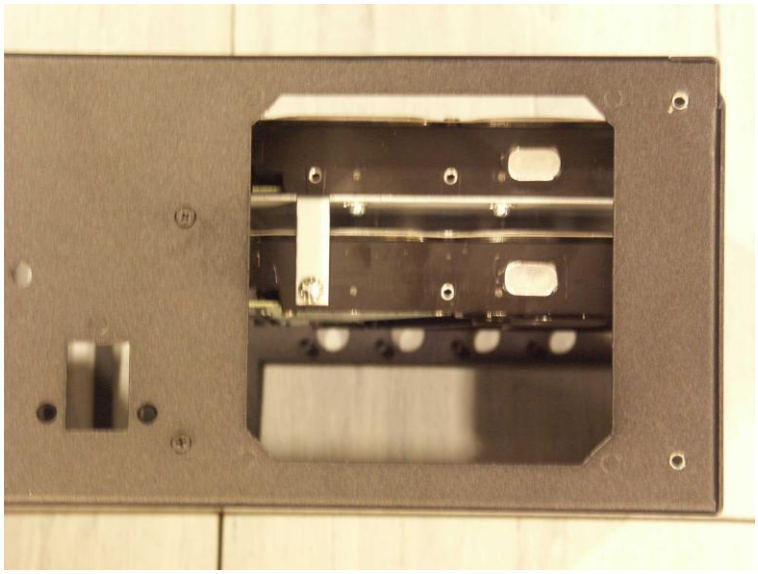
Fix the third disk on the topside of the third support (mount before the fourth).



Fix – if desired – the fourth disk on the bottom side of the same support.

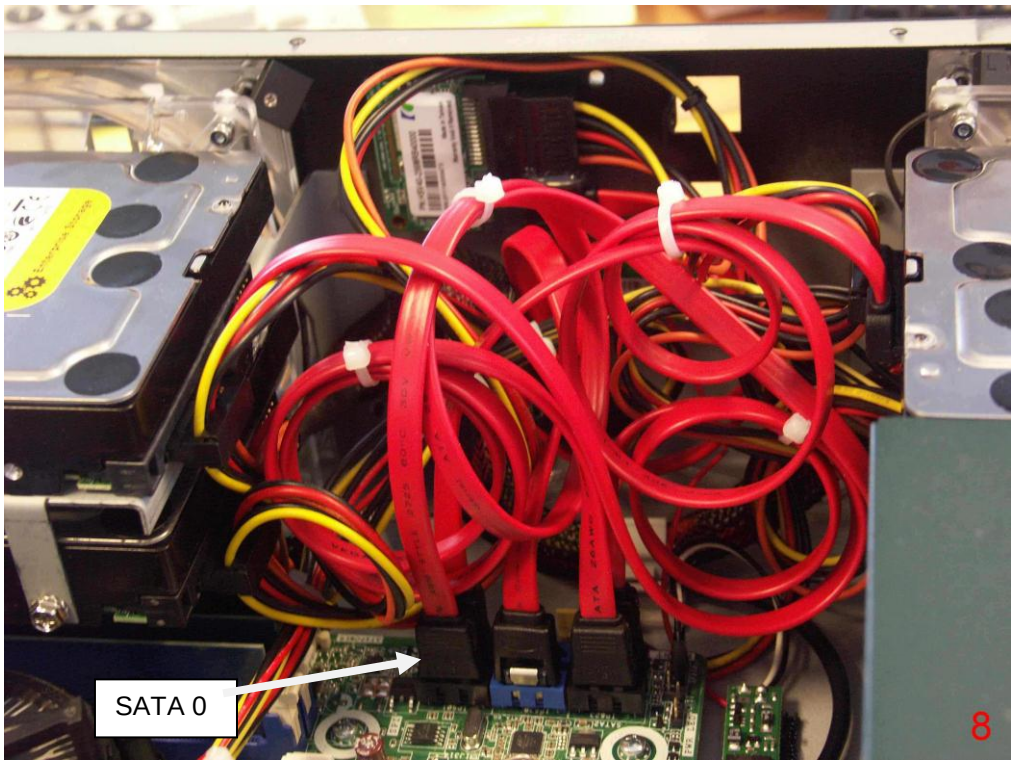


Install the support with two screws (# 17439080) at the front and on the right side of the casing.



Then connect disk 3 to SATA2 connector with the SATA cable (# 16520875).

When disk 4 is in use connect it to SATA3 connector with the SATA cable (# 16520875).



Pay attention: Do not bend the SATA cables too sharp to avoid cable damage!

Use tie-wraps to bundle the unused SATA power cables.

Then fix the front plate (# 17011610) on the base with the screws (# 17444080).
Put the cover in place and secure with 10 screws (# 17439080).

Connect monitor/screen and keyboard to the FastTrace 2 Server. Switch on power supply and define the BIOS settings for the FastTrace 2: choose **Boot** and then **Exit** (see FastTrace 2 BIOS settings). Wait for the boot window. Select **<FastTrace 2 Installer>** during startup. Next, select **Update current system > Manage recording disks** and select the new hard disk from the list. Press 'Enter'. Then select – use the TAB button – "**Format and use selected disk**". Select **Main Menu** and choose **Reboot**.

The video system will now reboot. After rebooting the new hard disk can be used.

Mind:

When using the ENTRY system license, only 1 hard disk can be used! This is for instance the case with the ADPRO FastTrace 2 Lite.

2.5 Fan speed selection

Two large fans are provided to dissipate the heat. The fans have a switch to select the speed: low, medium or fast. Whatever the ambient temperature, the fan speed may be set to **medium**. Only with extreme ambient temperatures the fan speed should be adapted.

2.6 Front LED indicators

On the front of the FastTrace 2 video system are 3 LEDs:

Green LED	⏻	Power is on
Yellow LED (*)	⚠	Fault
Blue LED	🛢	Storage media activity

Only the green and blue LED could be lit all the time. If you see the yellow LED lit, you should check the status of your FastTrace 2 video system.

(*) The yellow LED can only be lit when a Main I/O card has been installed.

Remark:

When the 3 LEDs are flashing simultaneously, the system is busy updating the recording discs. Do not turn off power in that case!

2.7 Required motherboard

The FastTrace 2 video system only operates with Intel DG31PR, Intel DG41TY, Intel DH55TC or Intel DH61BE motherboard.

Intel DG31PR motherboard	Intel DG41TY motherboard
Intel DH55TC motherboard	**Intel DH61BE motherboard**

2.7.1 FastTrace 2 BIOS settings

2.7.1.1 Motherboard Intel DG31PR or Intel DG41TY

Choose **Main > System Time** to set the system time.
Choose **Main > System Date** to set the system date.
Choose **Advanced > Numlock** and select the option ‘Off’.
Choose **Power > After Power Failure** and select the option ‘Power-On’.
Choose **Boot > Boot USB Devices First** and select the option ‘Enable’.
Choose **Exit > Exit & Save Changes** and select the option ‘Yes’.

All other parameters can be left to the default settings!

2.7.1.2 Motherboard Intel DH55TC

Choose **Main > System Time** to set the system time.
Choose **Main > System Date** to set the system date.
Choose **Advanced > Boot > Numlock** and select the option ‘Off’.
Choose **Advanced > Drive Configuration > Smart** and select the option ‘Disable’.
Choose **Advanced > Drive Configuration > Config AHCI** and select the option ‘On’.
Choose **Advanced > Event log > Event logging** and select the option ‘Disable’.
Choose **Advanced > Chipset Configuration > HPET** and select the option ‘Disable’.
Choose **Power > After Power Failure** and select the option ‘Power-On’.
Choose **Exit > Exit & Save Changes** and select the option ‘Yes’.

All other parameters can be left to the default settings!

2.7.1.3 Motherboard Intel DH61BE

Choose **Main > System Time** to set the system time.
Choose **Main > System Date** to set the system date.
Choose **Configuration > SATA drives > Smart** and select the option ‘Disable’.
Choose **Configuration > SATA drives > Chipset SATA mode** and select the option ‘AHCI’.
Choose **Configuration > Event log > Event logging** and select the option ‘Disable’.
Choose **Power > After Power Failure** and select the option ‘Power-On’.
Choose **Boot > Hard drive order** and place the DOM ‘CSS HSV40-256M’ at the top of the list, using the arrows to select the DOM and the + key to move the selected DOM upwards. Press ‘Enter’.
Choose **Exit > Exit & Save Changes** and select the option ‘Yes’.

All other parameters can be left to the default settings!

Important:

The BIOS settings need to be reset every time a hard disk is replaced or added with the Intel DH61BE motherboard!

2.7.2 Main & Extension I/O Cards

The OTB (On the board) I/O cards are internal I/O cards, to be fitted inside the ADPRO FastTrace 2 system.

These I/O cards offer:

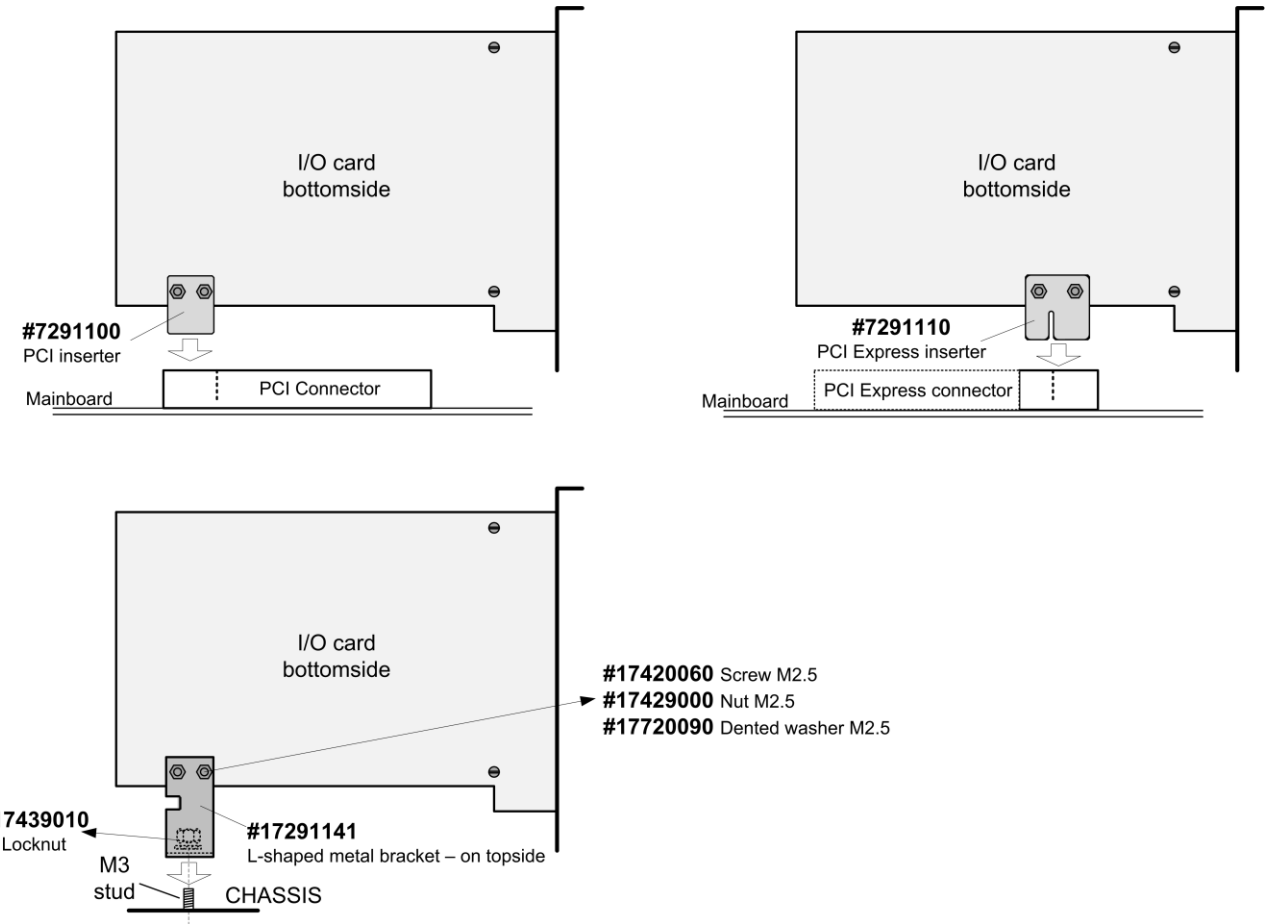
- 8 tamper protected inputs and 4 relay outputs (rated 30VDC @ 1A) on Main IO board;
- 12 tamper protected inputs and 4 relay outputs on Extension IO board;
- driver for PTZ cameras (half/full duplex RS485) or audio module / VM22A audio switcher (selected by straps on the card);
- driver for front LED indicators on FastTrace 2 model;
- auto-detected cards on FastTrace 2 system.

You can configure 2 sets maximum on the FastTrace 2:

- only Main I/O
- Main I/O + Extension I/O
- 2 x Main I/O + Extension I/O
- 2 x Main I/O + 2 x Extension I/O

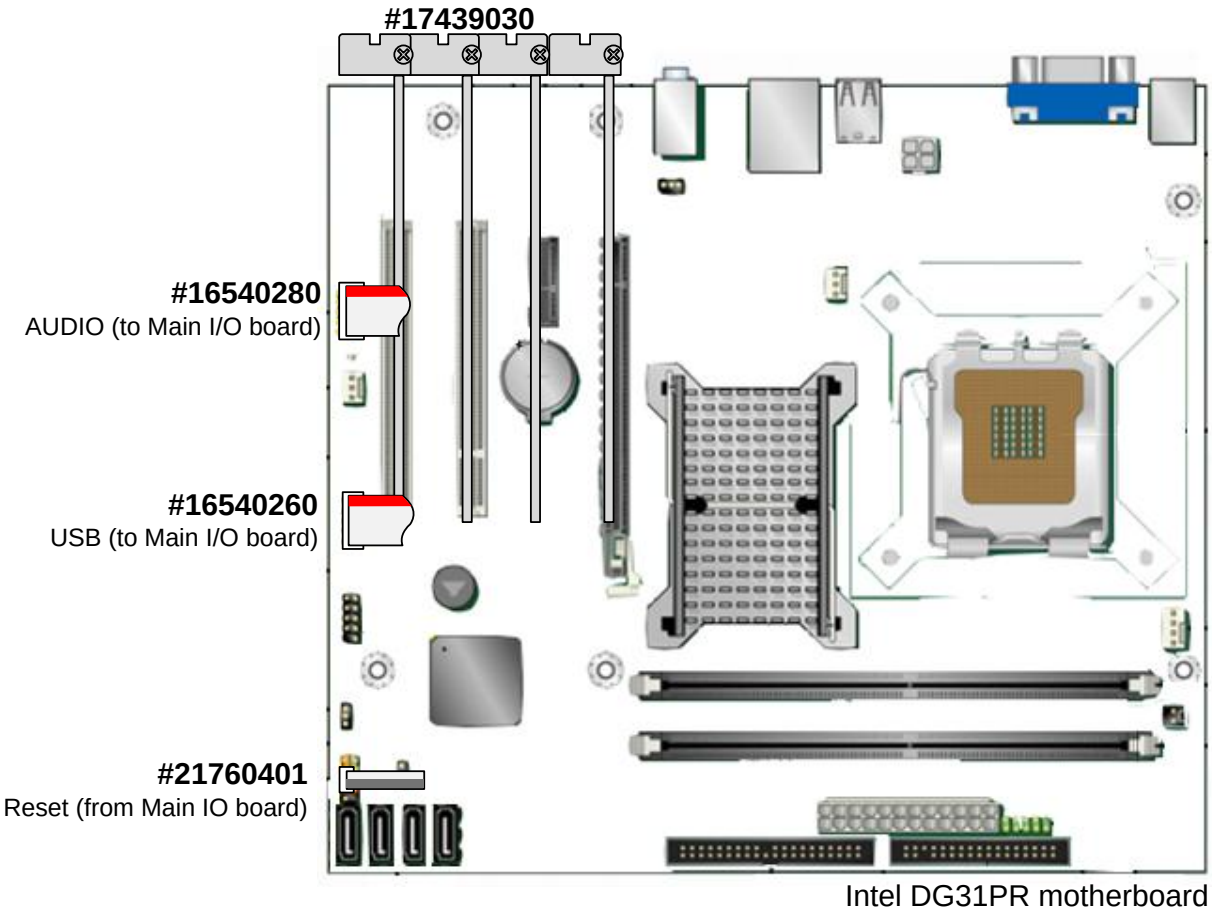
2.7.2.1 How to insert the I/O card?

The first set is inserted in the two furthermost slots (= nearest to the power supply) and fixed to the chassis applying the L shaped brackets. The Main I/O card is inserted in the furthermost slot (= slot 6).
The second set is inserted in the PCI or PCI Express slots using the included PCI or PCI Inserters.
Depending on the type of motherboard, you will need either a PCI or PCI Express Inserter.



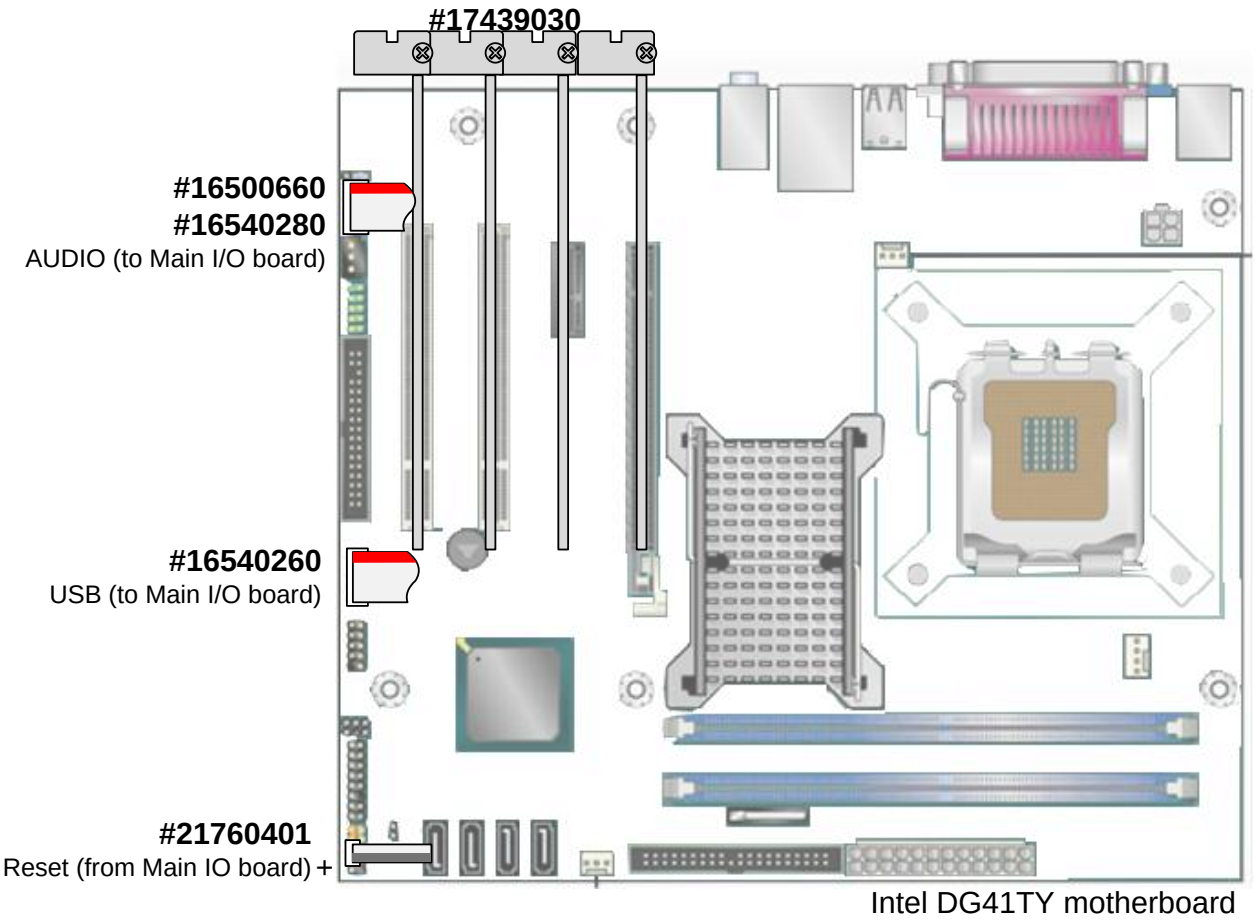
*Please also consult the technical data sheet on the **Main & Extension I/O cards**. (document reference 19531920)*
The reference numbers are the numbers you need for ordering with Xtralis.

2.7.2.1.1 Inserting the I/O cards on an Intel DG31PR motherboard



Intel DG31PR motherboard

2.7.2.1.2 Inserting the I/O cards on an Intel DG41TY motherboard

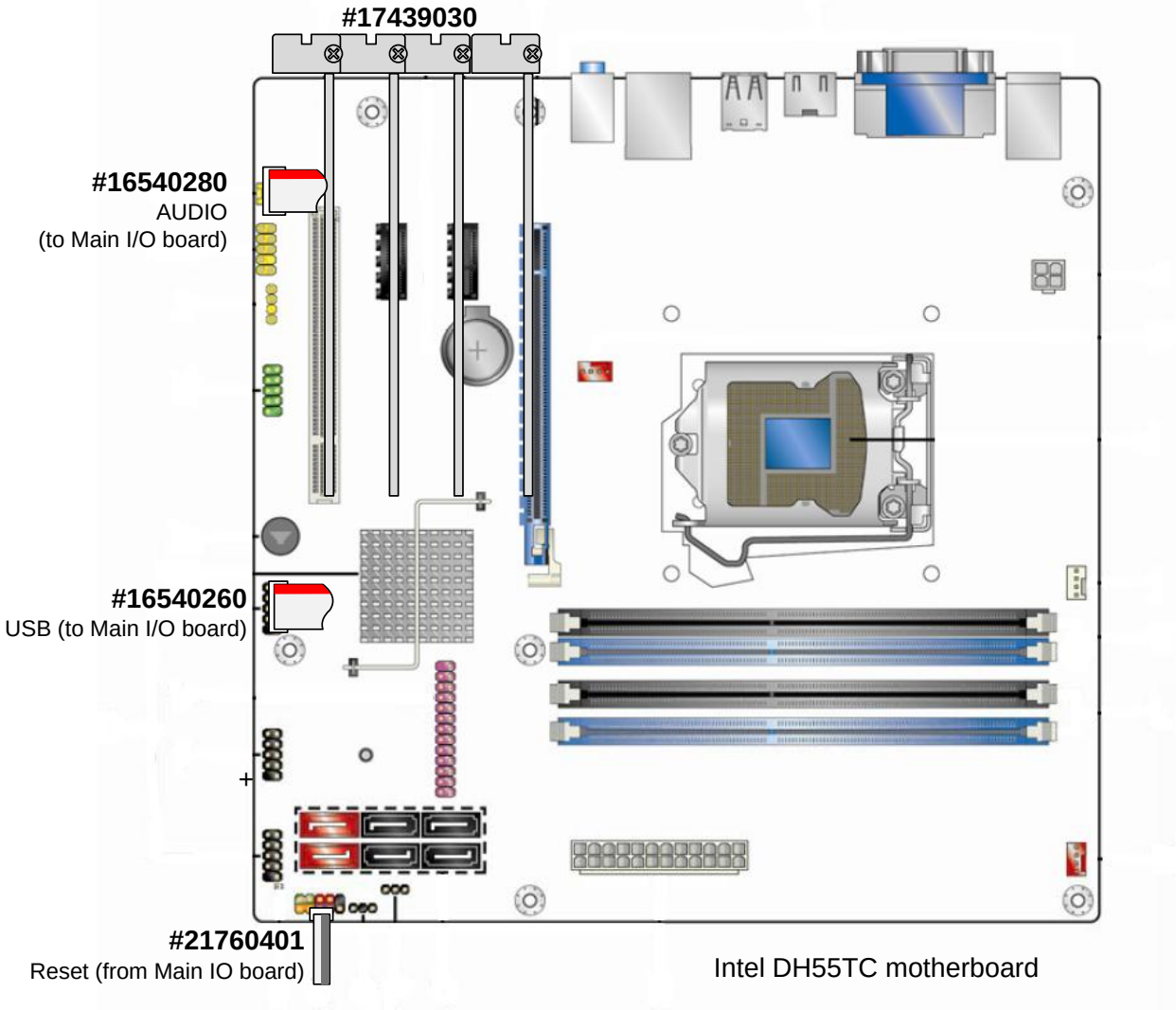


Intel DG41TY motherboard

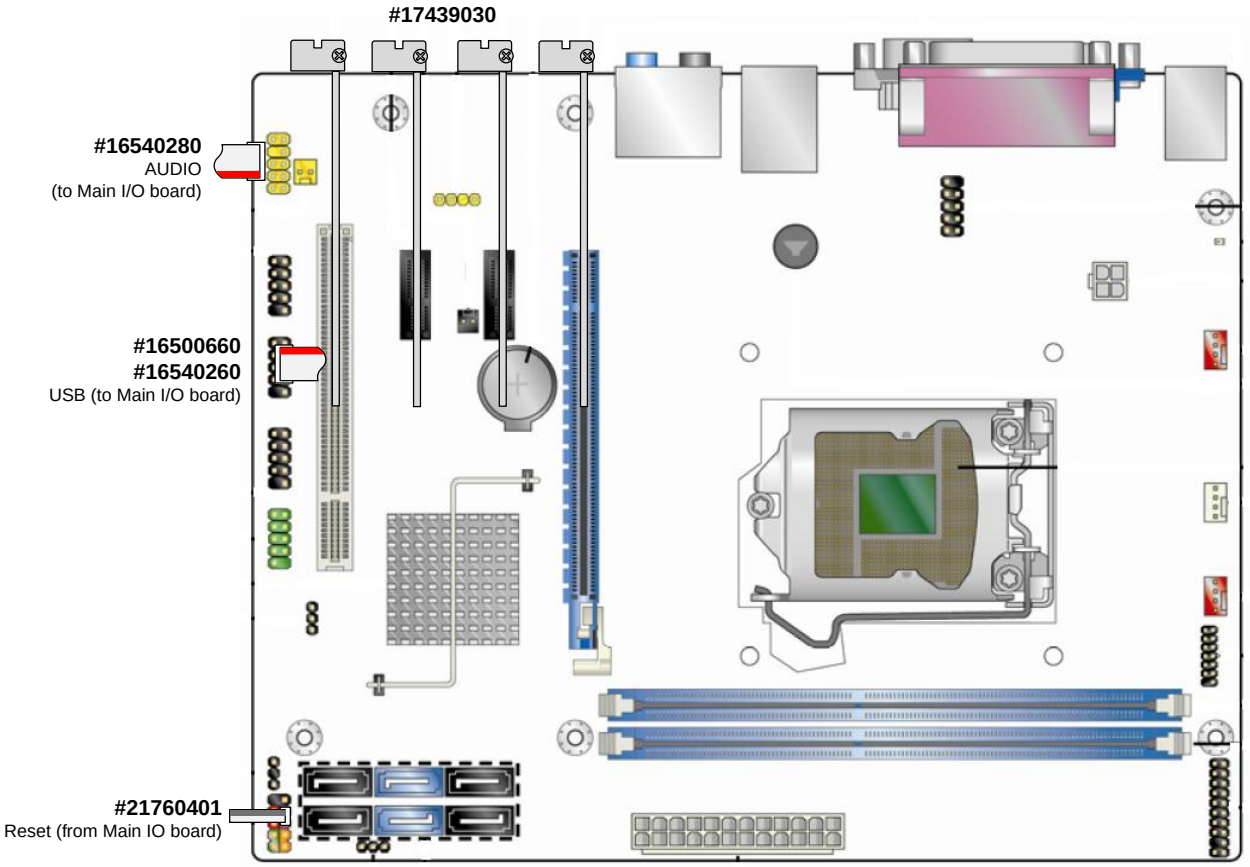
Mind:

An audio connector adapter (#16500660) is required with the Intel DG41TY motherboard to connect the flat cable to the motherboard. You need to order this audio connector adapter separately.

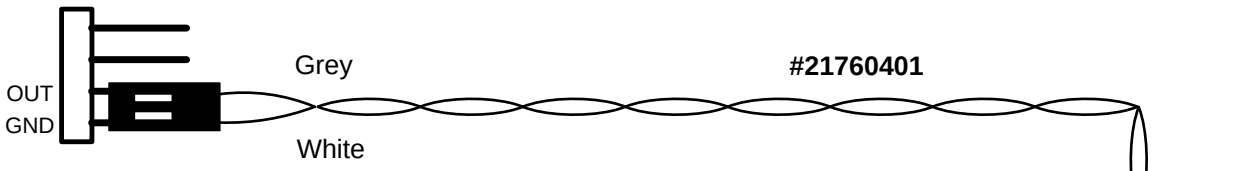
2.7.2.1.3 Inserting the I/O cards on an Intel DH55TC motherboard



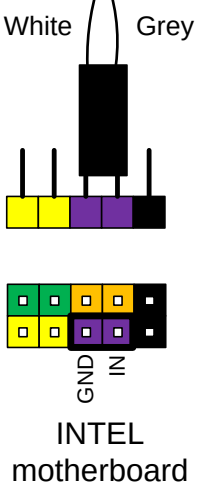
2.7.2.1.4 Inserting the I/O cards on an Intel DH61BE motherboard



2.7.2.1.5 Reset signal



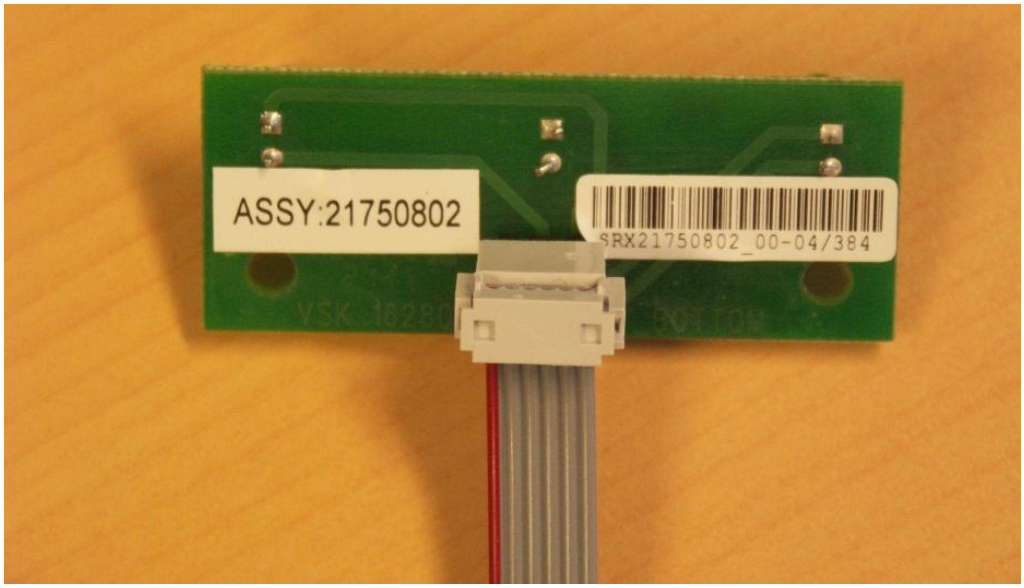
In case of a cable with two grey-coloured wires (older type), the right polarity should be checked visually or by means of a multimeter.
A reversed connection won't do any harm, but the motherboard receives a permanent reset signal!

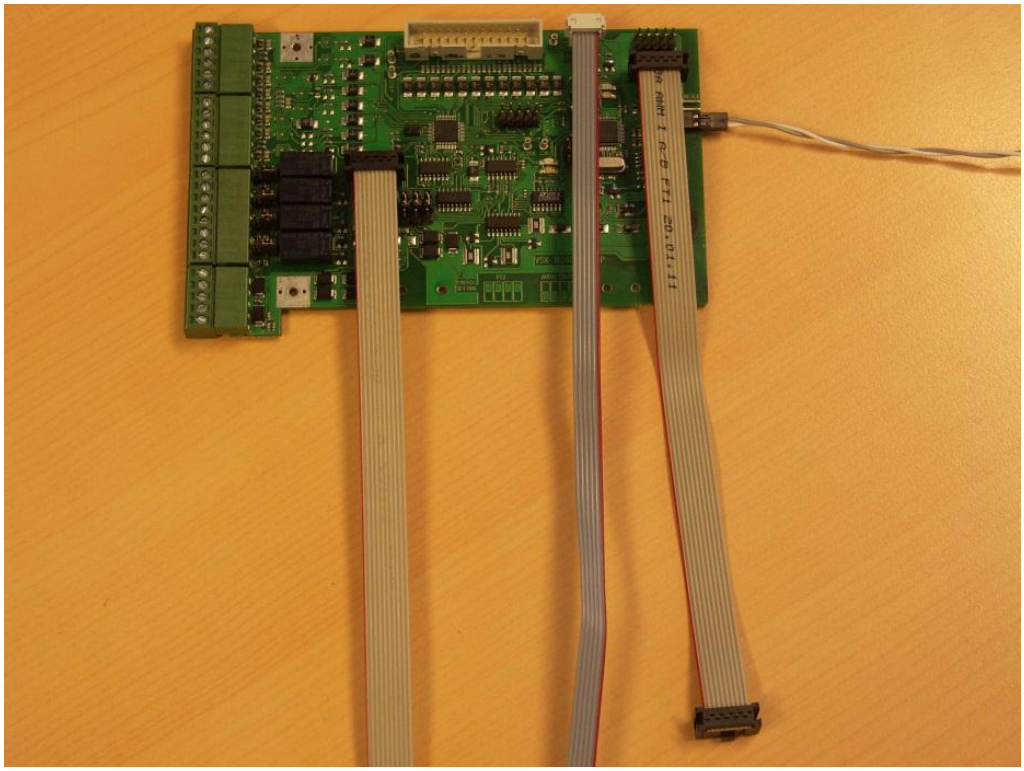


2.7.2.1.6 I/O cards with mounting sets

2.7.2.1.6.1 Mounting order

Remove the two cables connecting the LED board on the front to the motherboard. The LEDs will be powered from the Main I/O card (of the 1st set) when installing an I/O card. Insert the flat cable #21760101 in place of the removed cables.





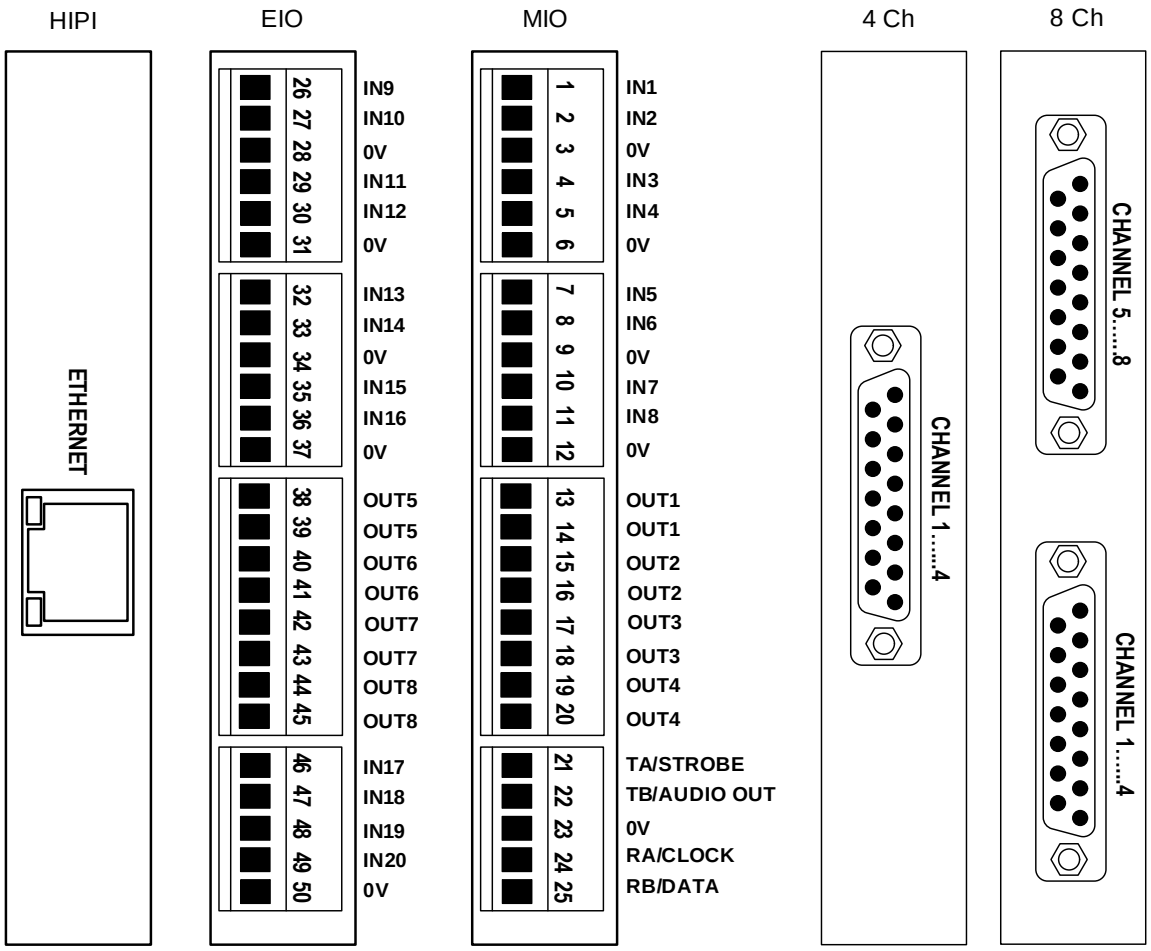
Before inserting the I/O cards into the motherboard, make sure you have connected all necessary cables to plug in the card into the motherboard. Remove any superfluous blind brackets.

2.7.3 Replacing the motherboard

The FastTrace 2 Server's motherboard should not be replaced in the field. When replacement of the motherboard is required, please send back the FastTrace 2 unit to your supplier.

2.8 Extension boards

Type	Description
HIPI	PCI Express extension board for 8 IP cameras. See also technical data sheet *19531930 – HIPI card*.
4ch/8ch DS40xx	PCI extension board for 4 or 8 analogue cameras, including audio inputs per camera ***Note**: these PCI Cards are to be used on an Intel DG31PR or Intel DG41TY motherboard!*
4ch/8ch DS42xx	PCI EXPRESS extension board for 4 or 8 analogue cameras, including audio inputs per camera ***Note**: these PCI Express Cards are to be used on an Intel Intel DH55TC motherboard!*
Main I/O	Main Input Output board: USB extension card, inserted in a free PCI or PCI Express connector. See also technical data sheet *19531920 – Main & Extension I/O Cards*.
Extension I/O	Extension Input Output board: extension board, inserted in a free PCI of PCI Express connector and linked to the Main I/O board, extending the number of inputs and outputs. See also technical data sheet *19531920 – Main & Extension I/O Cards*.



Please consult the ADPRO FastTrace 2 field alerts #1 and #2 for detailed information on upgrading older versions to the newest firmware!

General rules

The FastTrace 2 Video System offers 6 extension slots:

- On Intel DG31PR and Intel DG41TY motherboards: two PCI Express slots, two PCI slots and two physical slots.
- On Intel DH55TC and Intel DH61BE motherboards: three PCI Express slots, one PCI slot and two physical slots.

The HIPI cards can only be inserted in a PCI Express slot.

The A/V cards type DS40xx require a PCI slot. The A/V cards type DS42xx require a PCI Express slot. They also require different types of motherboard, so ***a mixture of DS40xx and DS42xx cards is not possible***!

Main I/O and Extension I/O cards can be inserted anywhere (in any free slot left unused); the MIO card is connected to an internal USB connector and the EIO card is connected to the MIO card through a flat cable.

2.8.1 Required video card

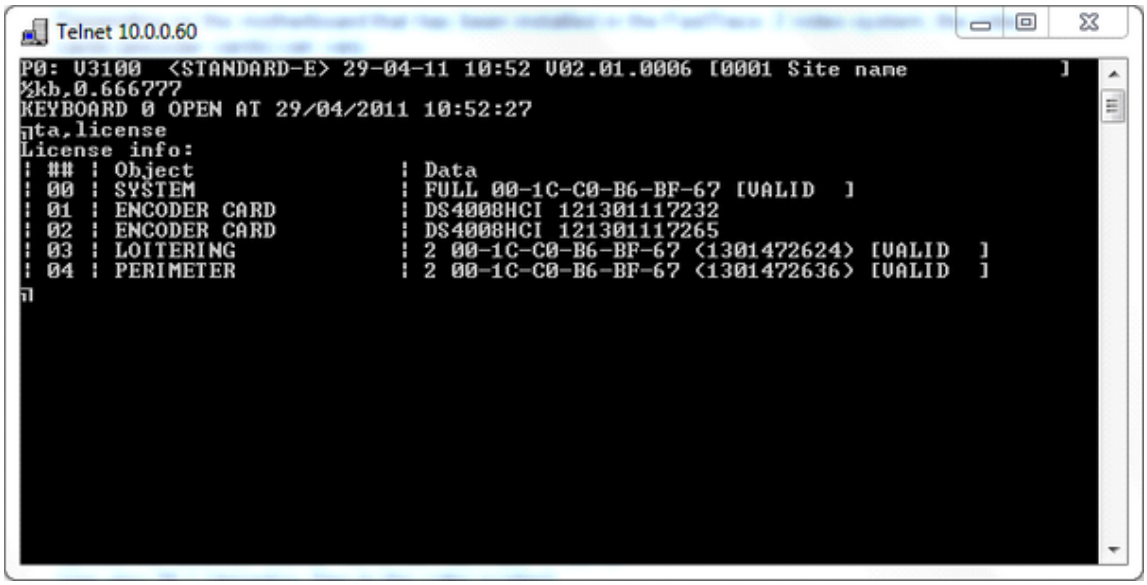
Depending on the motherboard that has been installed in the FastTrace 2 video system, the video cards (encoder cards) can vary:

- DS40xx-HCI encoder cards are used with Intel DG31PR and Intel DG41TY motherboards.
- DS42xx-HFVI-E encoder cards are used with the Intel DH55TC and Intel DH61BE motherboards.

The mixture of these two cards within the same video system is not supported!

2.8.1.1 Replacing a video card

First check your license (via a Telnet connection executing the command **ta,license**). If no license information is listed, your license may have been deleted (by accident). Contact your dealer for a new license.
(*see also* *License types*)


Telnet 10.0.0.60
P0: V3100 <STANDARD-E> 29-04-11 10:52 V02.01.0006 [0001 Site name]
%kb,0.666777
KEYBOARD 0 OPEN AT 29/04/2011 10:52:27
ta,license
License info:
| ## | Object | Data
| 00 | SYSTEM | FULL 00-1C-C0-B6-BF-67 [VALID]
| 01 | ENCODER CARD | DS4008HCI 121301117232
| 02 | ENCODER CARD | DS4008HCI 121301117265
| 03 | LOITERING | 2 00-1C-C0-B6-BF-67 (1301472624) [VALID]
| 04 | PERIMETER | 2 00-1C-C0-B6-BF-67 (1301472636) [VALID]

Trace the faulty video card by checking LIVE images of the connected cameras in the FastTrace 2 Client. Switch off power supply and remove the faulty video card. Insert the new video card in the slot where you removed the old one. It is recommended to return the faulty video card to your reseller!

Switch on power supply and reboot the video system. The replacement part will include a new license. Upload the received license file to the FastTrace 2 Server.
(*see also* *Uploading files to the video system*)

2.8.1.2 Adding a video card

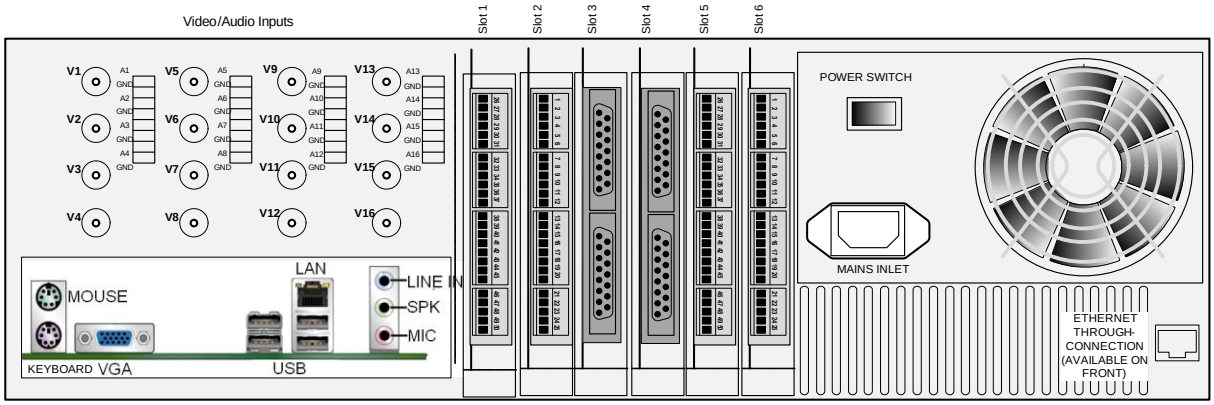
Switch off power supply. Open the casing and insert the new video card (in a free slot). Close the casing and switch on power supply. The new video card will include a new license on delivery. Upload the received license file to the FastTrace 2 Server.
(*see also* *Uploading files to the video system*)

2.8.2 DTC board

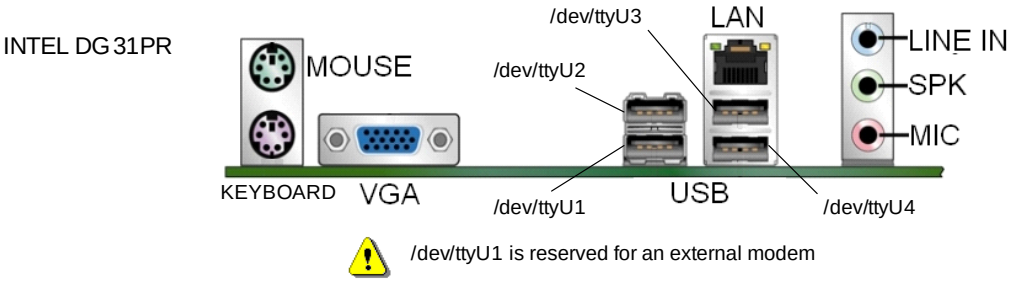
The DTC board offers ‘Down The Coax’ PTZ control. This board is inserted on the back of the audio/video connection board.

2.9 Available configurations

2.9.1 With Intel DG31PR motherboard



2.9.1.1 Network/monitor/keyboard



Mind:

USB input 1 (/dev/ttyU1) is reserved for an external modem!

2.9.1.2 Extension slots

Slot	Type	Accepts
1	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras
2	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras
3	PCI	- Main I/O - Extension I/O - A/V with 4 or 8 channels (lowest camera numbers: CAM 1 > 4/8)
4	PCI	- Main I/O - Extension I/O - A/V with 4 or 8 channels (highest camera numbers: CAM 5/9 > 8/16)
5	/	- Extension I/O
6	/	- Main I/O

2.9.1.3 The Xtralis configurations

2.9.1.3.1 Analogue cameras (4 – 8 – 12 – 16 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	Main I/O 2
3	PCI	A/V 4 channels 1 or A/V 8 channels 2
4	PCI	A/V 8 channels 1
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.1.3.2 IP Cameras (8 or 16 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	HIPI (ETH2)
3	PCI	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

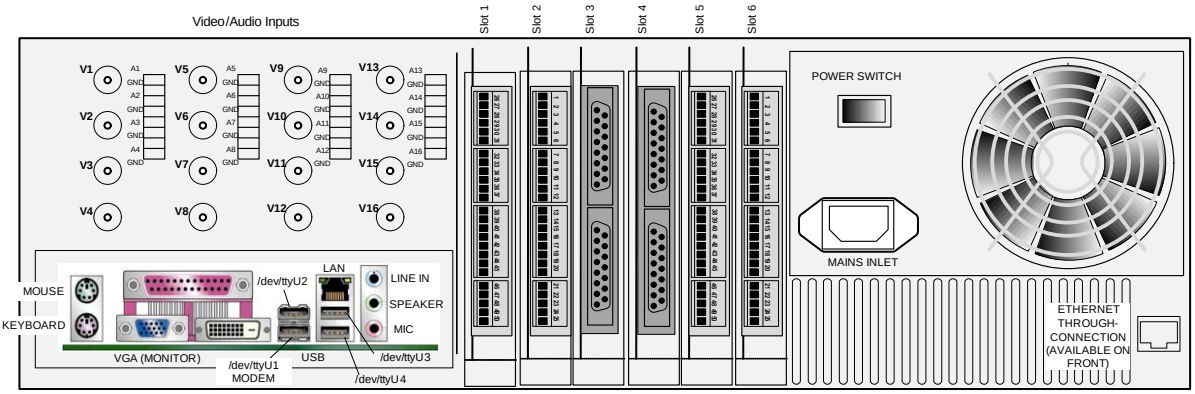
2.9.1.3.3 Hybrid (12 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI	A/V 4 channels 1
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

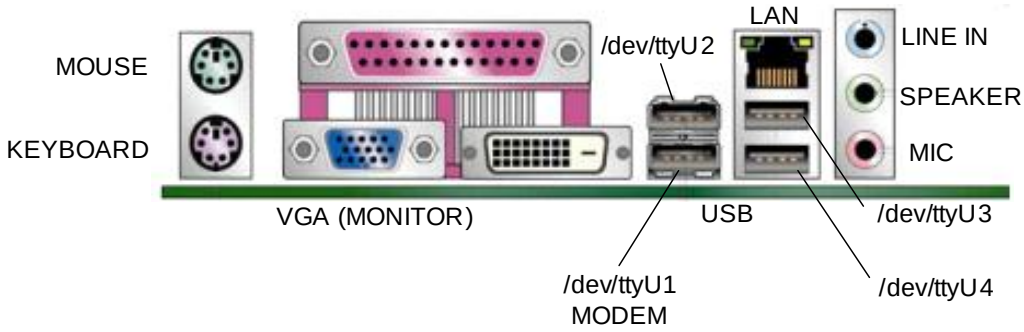
2.9.1.3.4 Hybrid (16 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI	Main I/O 2
4	PCI	A/V 8 channels 1
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.2 With Intel DG41TY motherboard



2.9.2.1 Network/monitor/keyboard



Mind:

USB input 1 (/dev/ttyU1) is reserved for an external modem!

2.9.2.2 Extension slots

Slot	Type	Accepts
1	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras
2	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras
3	PCI	- Main I/O - Extension I/O - A/V with 4 or 8 channels (lowest camera numbers: CAM 1 > 4/8)
4	PCI	- Main I/O - Extension I/O - A/V with 4 or 8 channels (highest camera numbers: CAM 5/9 > 8/16)
5	/	- Extension I/O
6	/	- Main I/O

2.9.2.3 The Xtralis configurations

2.9.2.3.1 Analogue cameras (4 – 8 – 12 – 16 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	Main I/O 2
3	PCI	A/V 4 channels 1 or A/V 8 channels 2
4	PCI	A/V 8 channels 1
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.2.3.2 IP Cameras (8 or 16 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	HIPI (ETH2)
3	PCI	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

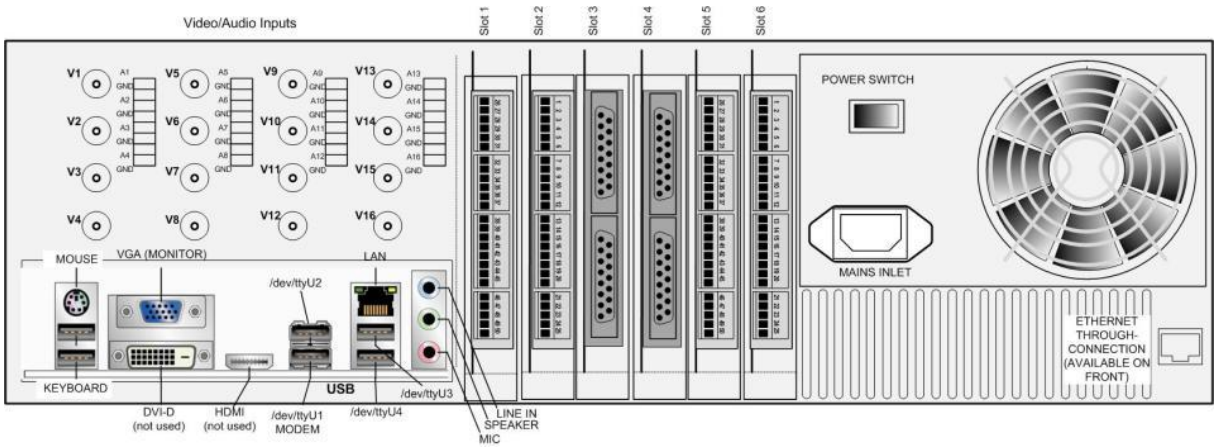
2.9.2.3.3 Hybrid (12 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI	A/V 4 channels 1
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

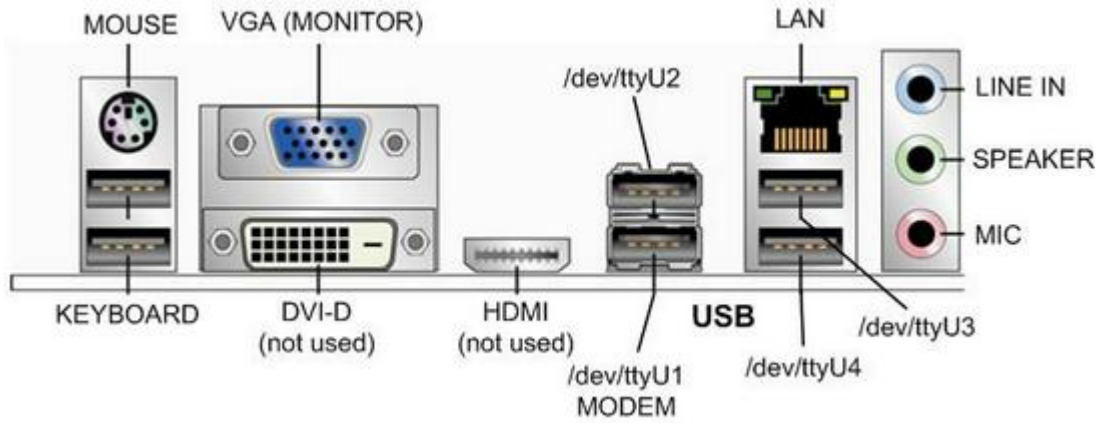
2.9.2.3.4 Hybrid (16 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI	A/V 8 channels 1
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3 With Intel DH55TC motherboard



2.9.3.1 Network/monitor/keyboard



Mind:

USB input 1 (/dev/ttyU1) is reserved for an external modem!

2.9.3.2 Extensions slots

Slot	Type	Accepts
1	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras - A/V with 4 or 8 channels
2	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras - A/V with 4 or 8 channels
3	PCI Express	- Main I/O - Extension I/O - A/V with 4 or 8 or 16 channels
4	PCI	- Main I/O - Extension I/O
5	/	- Main I/O - Extension I/O
6	/	- Main I/O - Extension I/O

When using A/V cards of equal A/V inputs the lowest camera numbers should be attributed to the A/V card that is in or closest to slot 1.

When combining a 4CH and an 8CH A/V card, the lowest camera numbers must be attributed to the lowest A/V card density. Example: camera numbers 1 through 4 allocated to the 4CH A/V card and numbers 5 through 12 allocated to the 8CH A/V card.

2.9.3.3 The Xtralis configurations

2.9.3.3.1 Analogue cameras (4 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	A/V 4 channels 1 (DS42xx)
3	PCI Express	
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.2 Analogue cameras (8 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	A/V 8 channels 1 (DS42xx)
3	PCI Express	
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.3 Analogue cameras (12 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	A/V 4 channels 1 (DS42xx)
3	PCI Express	A/V 8 channels 1 (DS42xx)
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.4 Analogue cameras (16 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	
3	PCI Express	A/V 16 channels 1 (DS42xx)
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.5 IP Cameras (8 or 16 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	HIPI (ETH2)
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.6 Hybrid (12 channels)

Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI Express	A/V 4 channels 1
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.3.3.7 Hybrid (16 channels)

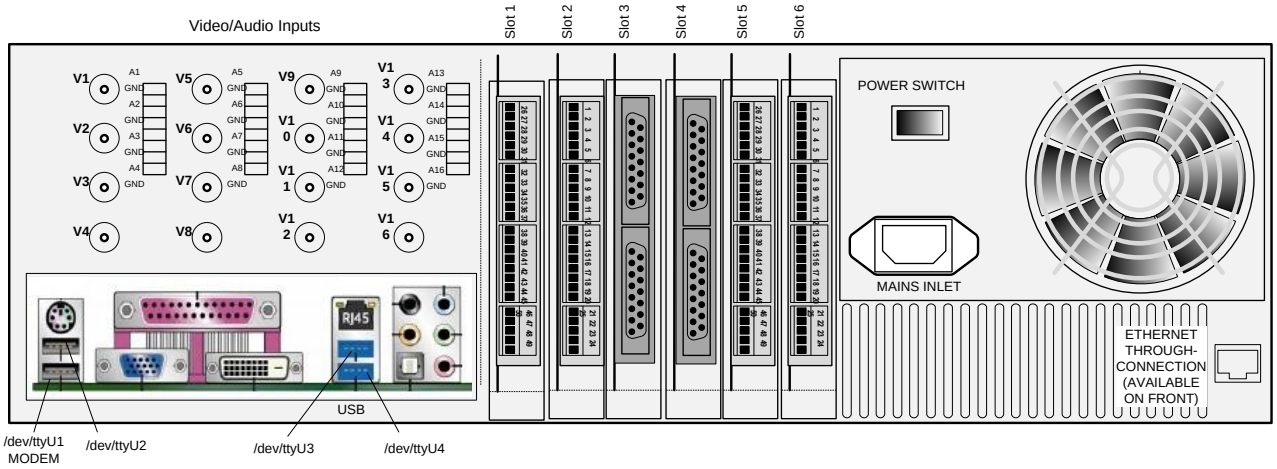
Slot	Type	Extension card
1	PCI Express	HIPI (ETH1)
2	PCI Express	Extension I/O 2
3	PCI Express	A/V 8 channels 1
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

A sticker below each slot, visible from the back of the appliance, indicates which card has been installed at that position.

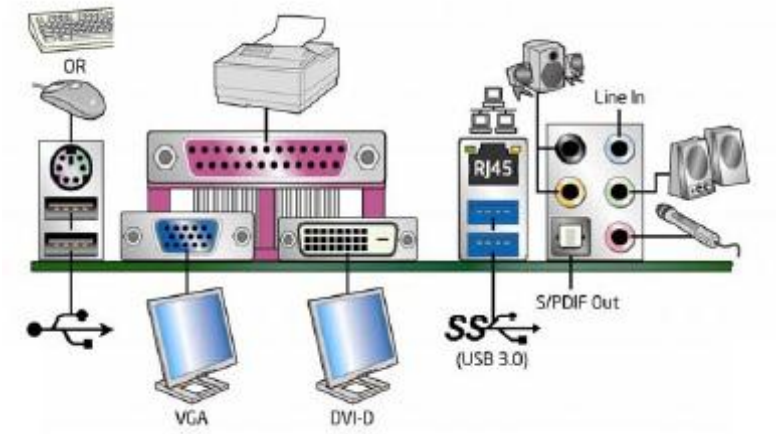
Mind:

Only the A/V cards type DS42xx are allowed on the Intel DH55TC motherboard!

2.9.4 With Intel DH61BE motherboard



2.9.4.1 Network/monitor/keyboard



Mind:

USB input 1 (/dev/ttyU1) is reserved for an external modem!

2.9.4.2 Extensions slots

Slot	Type	Accepts
1	PCI Express	- Main I/O - Extension I/O - A/V with 4 or 8 or 16 channels
2	PCI Express	- Main I/O - Extension I/O - HIPI (ETH1) for 8 IP cameras - A/V with 4 or 8 channels
3	PCI Express	- Main I/O - Extension I/O - HIPI (ETH2) for 8 IP cameras - A/V with 4 or 8 channels
4	PCI	- Main I/O - Extension I/O
5	/	- Main I/O - Extension I/O
6	/	- Main I/O - Extension I/O

When using A/V cards of equal A/V inputs the lowest camera numbers should be attributed to the A/V card that is in or closest to slot 1.

When combining a 4CH and an 8CH A/V card, the lowest camera numbers must be attributed to the lowest A/V card density. Example: camera numbers 1 through 4 allocated to the 4CH A/V card and numbers 5 through 12 allocated to the 8CH A/V card.

2.9.4.3 The Xtralis configurations

2.9.4.3.1 Analogue cameras (4 channels)

Slot	Type	Extension card
1	PCI Express	A/V 4 channels 1 (DS42xx)
2	PCI Express	
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.2 Analogue cameras (8 channels)

Slot	Type	Extension card
1	PCI Express	A/V 8 channels 1 (DS42xx)
2	PCI Express	
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.3 Analogue cameras (12 channels)

Slot	Type	Extension card
1	PCI Express	A/V 4 channels 1 (DS42xx)
2	PCI Express	A/V 8 channels 1 (DS42xx)
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.4 Analogue cameras (16 channels)

Slot	Type	Extension card
1	PCI Express	A/V 16 channels 1 (DS42xx)
2	PCI Express	
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.5 IP Cameras (8 or 16 channels)

Slot	Type	Extension card
1	PCI Express	Extension I/O 2
2	PCI Express	HIPI (ETH1)
3	PCI Express	HIPI (ETH2)
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.6 Hybrid (12 channels)

Slot	Type	Extension card
1	PCI Express	A/V 4 channels 1
2	PCI Express	HIPI (ETH1)
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

2.9.4.3.7 Hybrid (16 channels)

Slot	Type	Extension card
1	PCI Express	A/V 8 channels 1
2	PCI Express	HIPI (ETH1)
3	PCI Express	Extension I/O 2
4	PCI	Main I/O 2
5	/	Extension I/O 1
6	/	Main I/O 1

A sticker below each slot, visible from the back of the appliance, indicates which card has been installed at that position.

Mind:

Only the A/V cards type DS42xx are allowed on the Intel DH61BE motherboard!

2.10 Network load

Application		**Bandwidth volume**
Alarm transmission		Negligible
Remote control (executing commands)		Negligible
Software update		Volume of about 170 MB
Configuration update		Volume of 150 kB
Video streaming	4CIF / 25 ips	400 kbps / camera
	4CIF / 6 ips	140 kbps / camera
	CIF / 25 ips	80 kbps / camera
	CIF / 6 ips	43 kbps / camera
	QCIF / 25 ips	17 kbps / camera
	QCIF / 6 ips	6 kbps / camera
Audio in		16 kbps / camera (with DS40xx cards) 64 kbps / camera (with DS42xx cards)
Audio out		8 kbps

Video streaming H.264, VBR, quality set to medium.

2.11 Current consumption

Estimated current consumption depends on which components have been installed and on the system load:

Motherboard	16W (Intel)
Processor	25W (AMD) with Intel DG31, DG41 and DH61 until 65W max; with Intel DH55 until 73W max.
4 channel A/V card	3,5W
8 channel A/V card	7W
Western digital RE hard disk	11W
Western digital RE2 hard disk	12W
Main I/O card	1W
Extension I/O card	1W
HIPI card (for IP cameras)	3W
DTC card (“Down the Coax”)	0,5W

Example (with maximum values):

Motherboard	16W
Processor	65W (DH61BE with G850 microprocessor)
two 8-channels V/A cards	14W
4 Western digital RE2 hard disks	48W
Main I/O card	1W
Extension I/O card	1W
TOTAL on secondary circuit on primary circuit *(total current consumption divided by 0.8 – this is the efficiency of the power supply)*	 155W 180W (0,80 A / 230 VAC)

Note:

Measurement on a fully equipped (*) FastTrace 2 server (with DH61BE motherboard and G850 microprocessor) came up with the following results: 0.41 A on 230 VAC ➞ 95 W (idle state)

(*) Fully equipped = FastTrace 2 server with 2 Main I/O cards, 1 Extension I/O card, 1 HIPI card, 2 8-channel A/V cards and 4 hard disks (2 TB per disk).

2.12 Maintenance

2.12.1 Replacing the filters

It is essential that the filters are regularly cleaned and – when needed – replaced by new filters.

You will need an Allen wrench (3 mm) to remove the front plate of the Fasttrace 2 server. Remove the screws indicated on the image below by the grey arrows and remove the front plate. Remove the dirty filters and replace them by clean ones (or new filters). Make sure the filters are placed straight with the borders behind the chassis before putting the front plate back in place. There should be no filter material stuck between the front plate and the chassis!

Put back the screws in place and pay attention to the USB slot (indicated by the red arrow). The USB slot needs to be accessible!

2.12.2 Cleaning the FastTrace 2 server

Cleaning the FastTrace 2 with water or any corrosive products is firmly NOT advised. Only dust cloths and wipes should be used when cleaning the outside of the FastTrace 2 server.

2.12.3 Replacing the motherboard battery

It might be necessary to replace the motherboard battery after some time of specific battery faults. Please consult the technical documentation of the specific motherboard for further instructions.

3 Client Setup and Configuration

3.1 Client software - minimum system requirements

3.1.1 Hardware

- Pentium 4; 1,6 GHz
- 512 MB RAM
- Graphics card that is compatible with DirectX 7.
  It is recommended to use a graphics card that allows YUV surfaces and hardware stretching. If not compatible the FastTrace 2 client software will force the graphics card to GDI mode, which will increase CPU load.

These minimum system requirements enable you to configure the FastTrace 2 video system from the Client software. Yet, if you want to use HD cameras in optimal quality, these requirements will prove insufficient. Please take into account that double resolution, on average, results in 4 times more performance.

It is advised to test the settings to make sure that your PC can handle your configuration!

3.1.2 Software

- Windows XP (SP2) or higher
- Internet Explorer 7 or higher
- DirectX 7

The FastTrace 2 Client version 2.01.xxxx is backwards compatible with all V3100 Hybrid versions (from version 2.00.xxxx) and all V3100 FT versions (from version 1.00.0001). However, some menu windows will look different, depending on the connected video system and the licenses that have been uploaded.

Remark:

It is recommended to install the latest drivers of your graphics card!

For NVIDIA cards please check the website http://www.nvidia.com.
For ATI cards please check the website http://ati.amd.com.

The client can always be forced into GDI mode. Add the line ‘gdi=1’ in the [General] section of the ‘hydra.ini’ file. This file can be found in your local work folder (of the FastTrace 2 application). Forcing the client to GDI mode is not recommended!

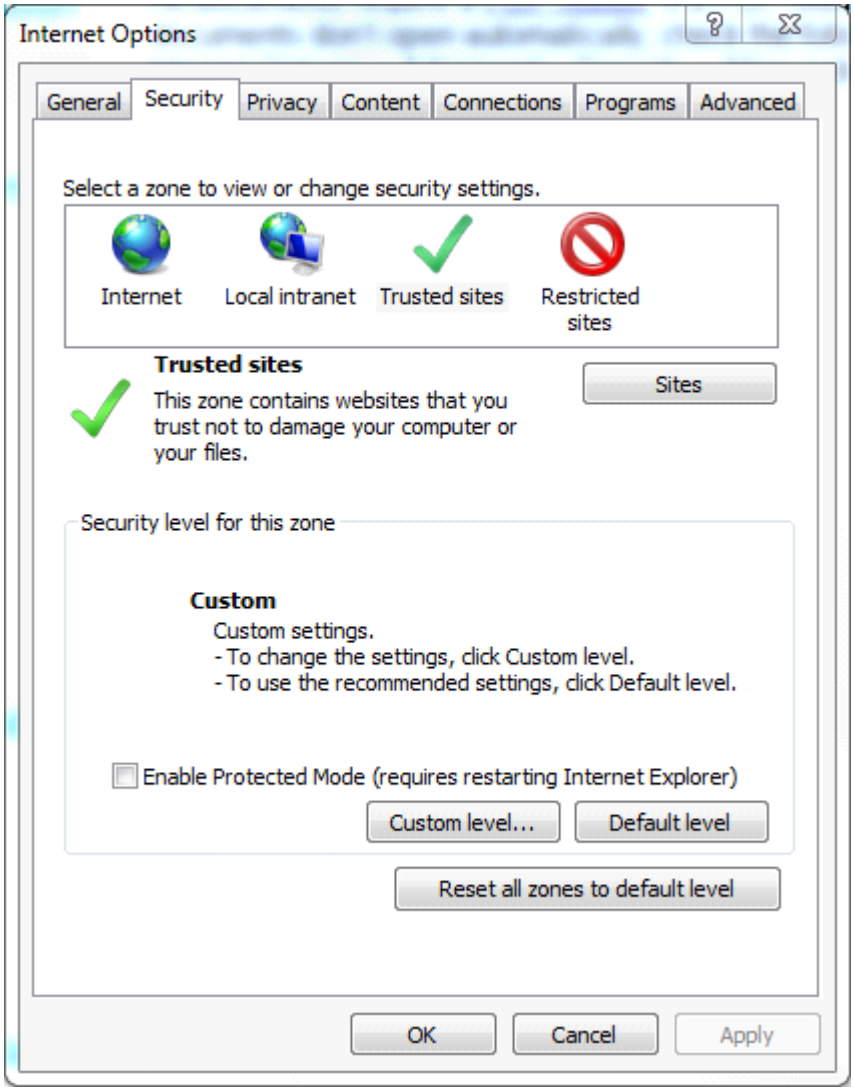
Installation of the **FastTrace 2 client software** is preferably done with **Internet Explorer**. If you can’t use Internet Explorer, try any other internet browser.

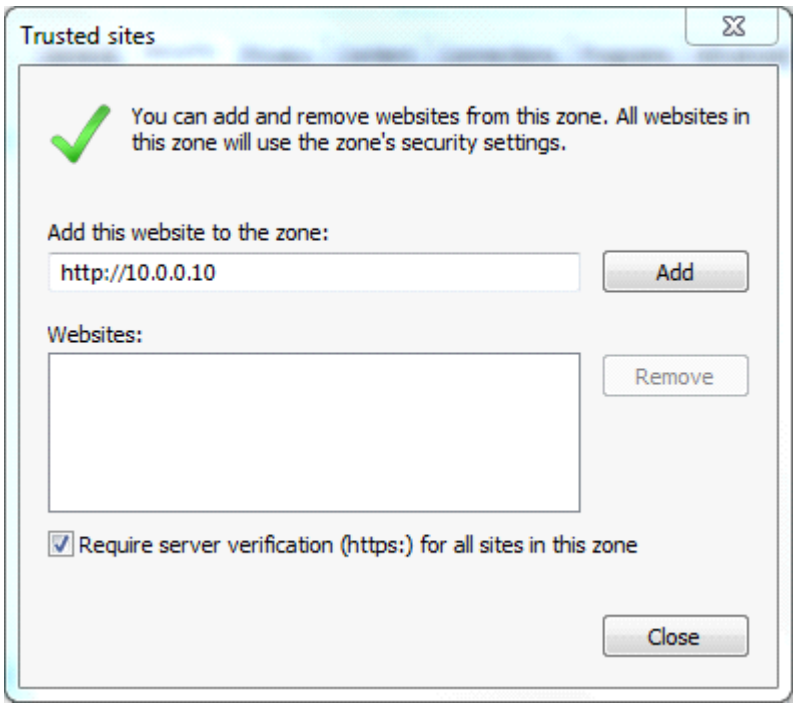
When installing the FastTrace 2 client software on a **Windows Vista** or **Windows 7** operating system, you need to add the FastTrace 2 IP address to your “Trusted Zones”. To add the IP address to the “Trusted Zones”, open **Internet Explorer > Tools > Internet Options > Security** and add the IP address.

3.2 Preparing your PC for installation

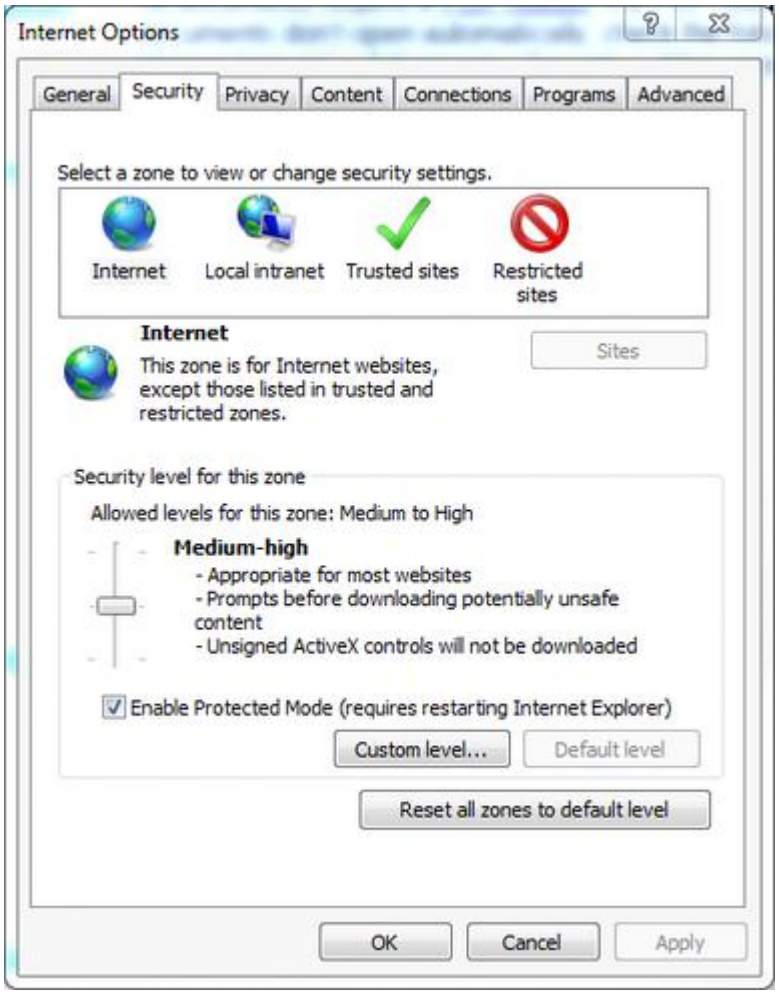
3.2.1 Internet Explorer Settings

To install the software on your PC your internet browser has to allow installation. We recommend using Internet Explorer for installation. You need to add the IP address of the FastTrace 2 Server as *trusted site* in Internet Explorer:




Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
http://10.0.0.10
Add
Websites:
Remove
Require server verification (https:) for all sites in this zone
Close

If this doesn't work, try switching off 'Protected Mode' via Internet Explorer > Tools > Internet Options > Security.



Please check with the IT department if you want to do this, because this might provide IT issues!

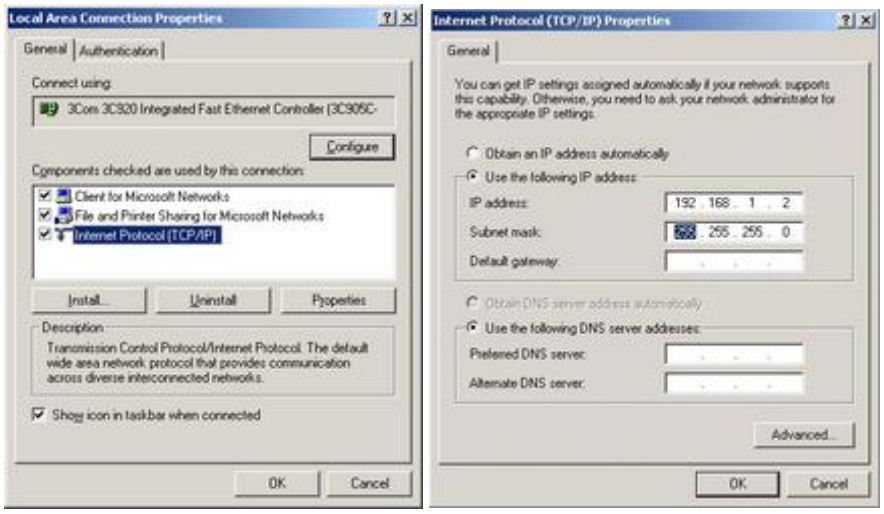
3.2.2 Changing the PC's IP address

The FastTrace 2 video system is by default on IP address 10.0.0.10 with subnet mask 255.255.255.0. When installing the client software, you need to put your PC in the same IP range (e.g. IP address 10.0.0.2 with subnet mask 255.255.255.0).

3.2.2.1 For Windows XP

From Start > All Programs > Accessories > Communications > Network Connections right click on **Local Area Connection** and select **Properties**.

From here, select Internet Protocol (TCP/IP) and click Properties:


Local Area Connection Properties
General
Authentication
Connect using:
3Com 3C920 Integrated Fast Ethernet Controller (3C905C-
Configure
Components checked are used by this connection:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in taskbar when connected
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

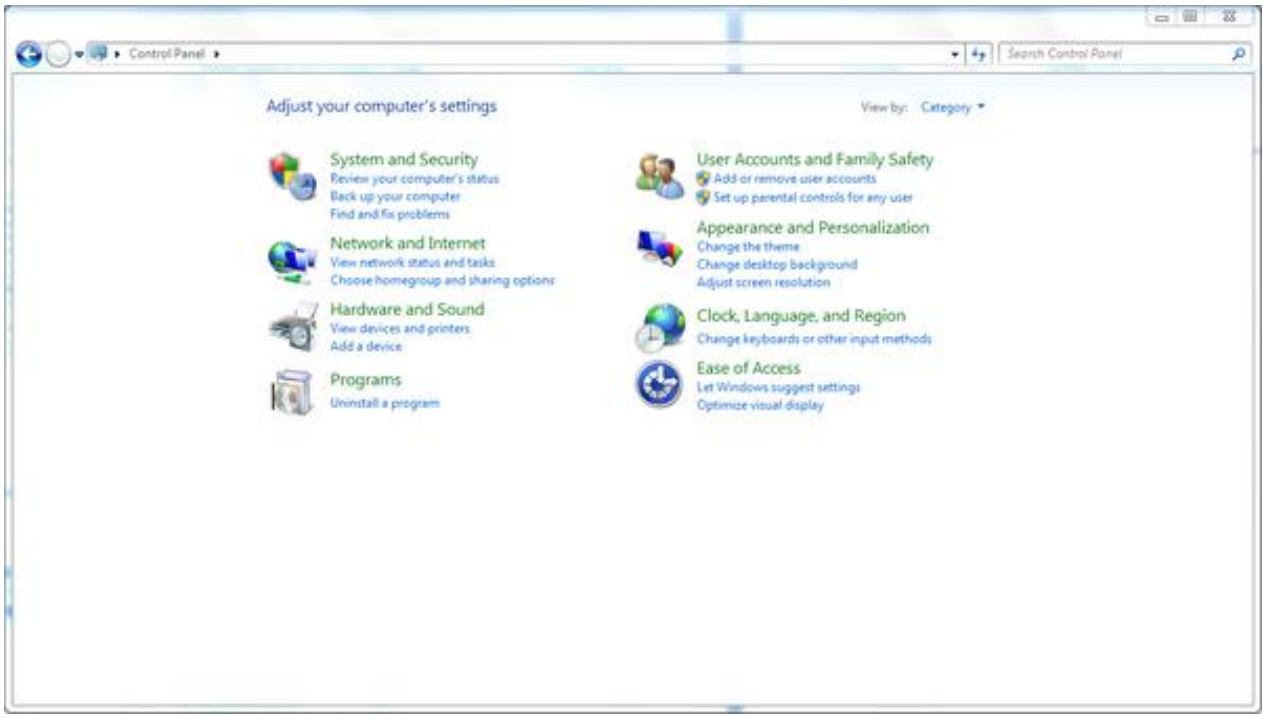
For ease of initial setup, you should change the PC's TCP/IP settings to the following:

IP address	10.0.0.2
Subnet mask	255.255.255.0

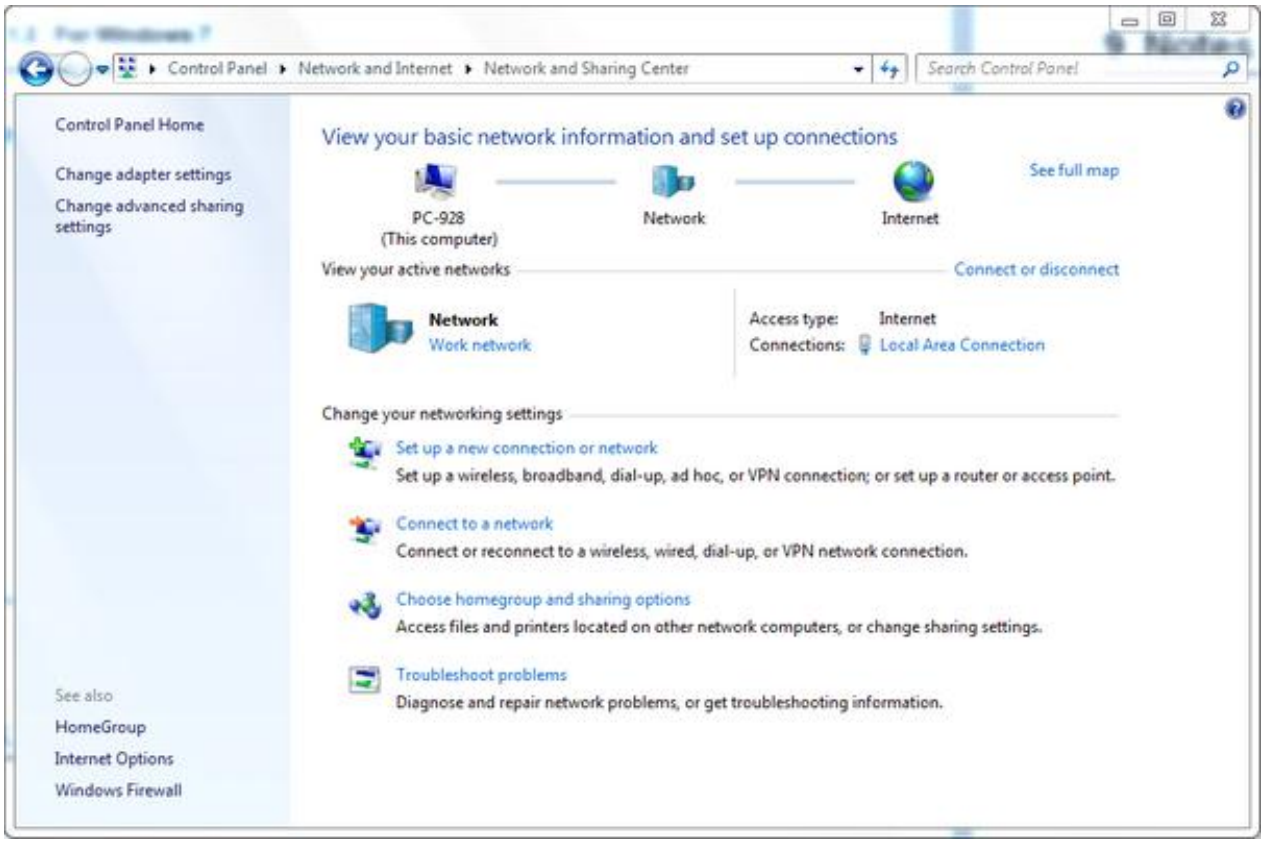
Click OK and the **Local Area Connection Properties** box is displayed again. Click **OK** and close the Network and Dial-up Connections panel.

3.2.2.2 For Windows 7

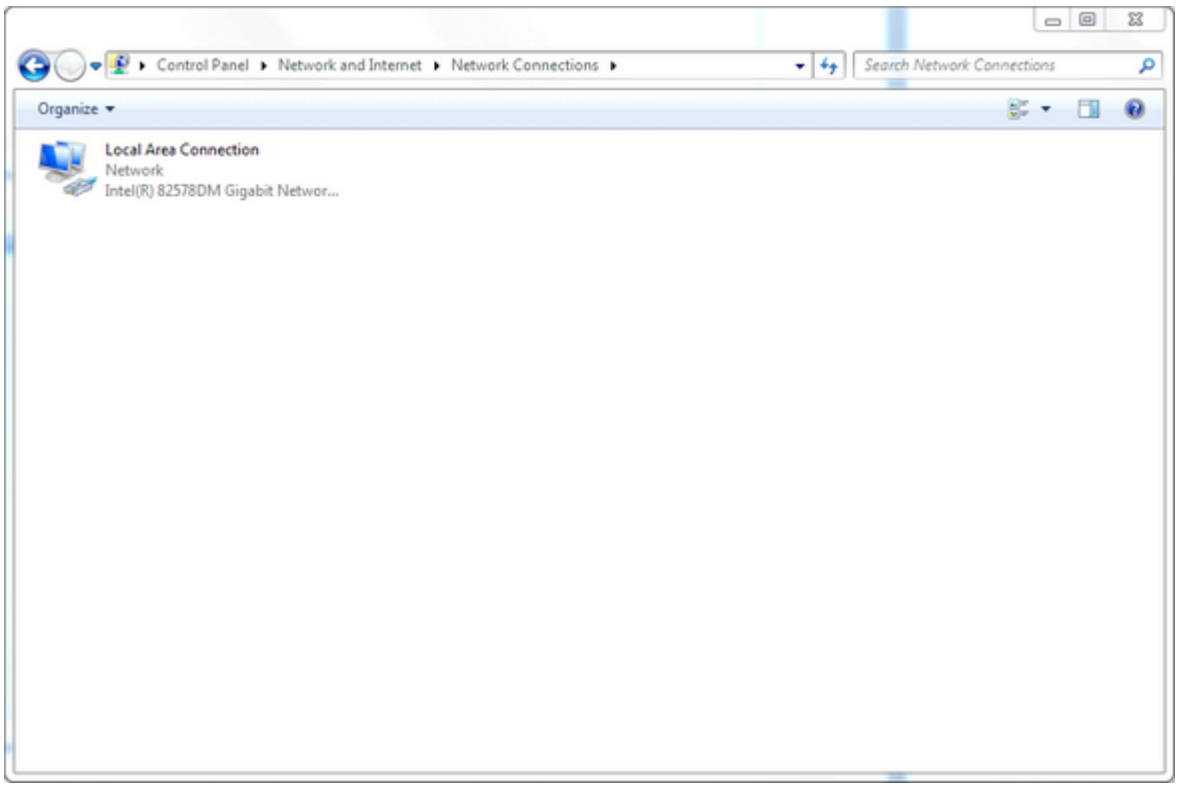
From **Start** click **Control Panel** (View by Category).



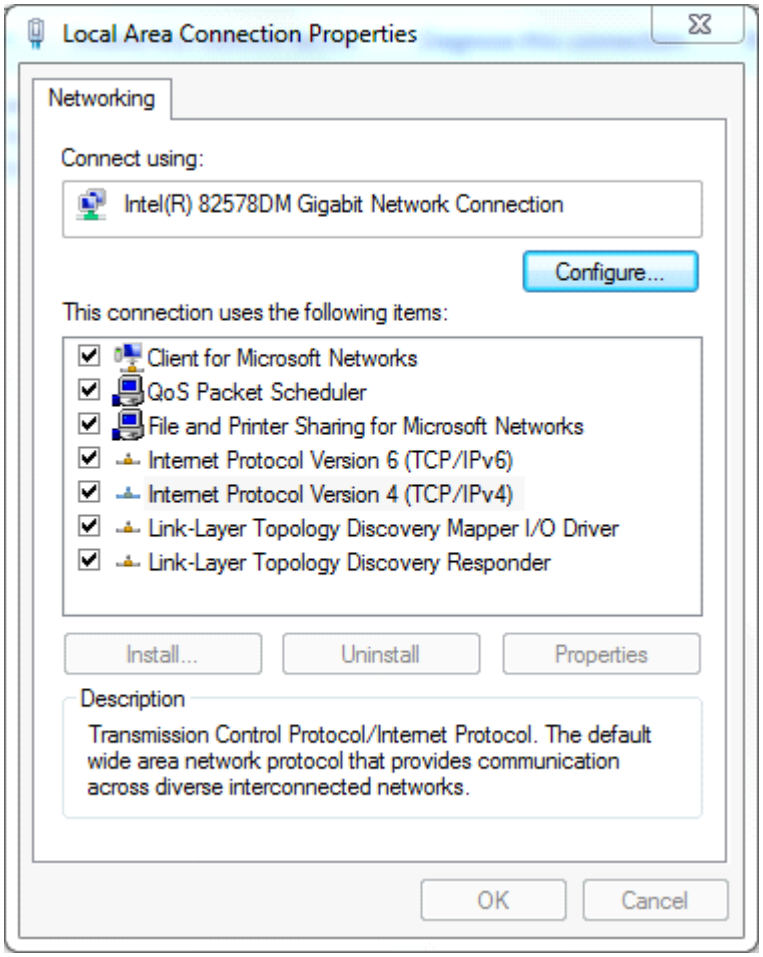
Click **Network and Internet**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
PC-928
(This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Work network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

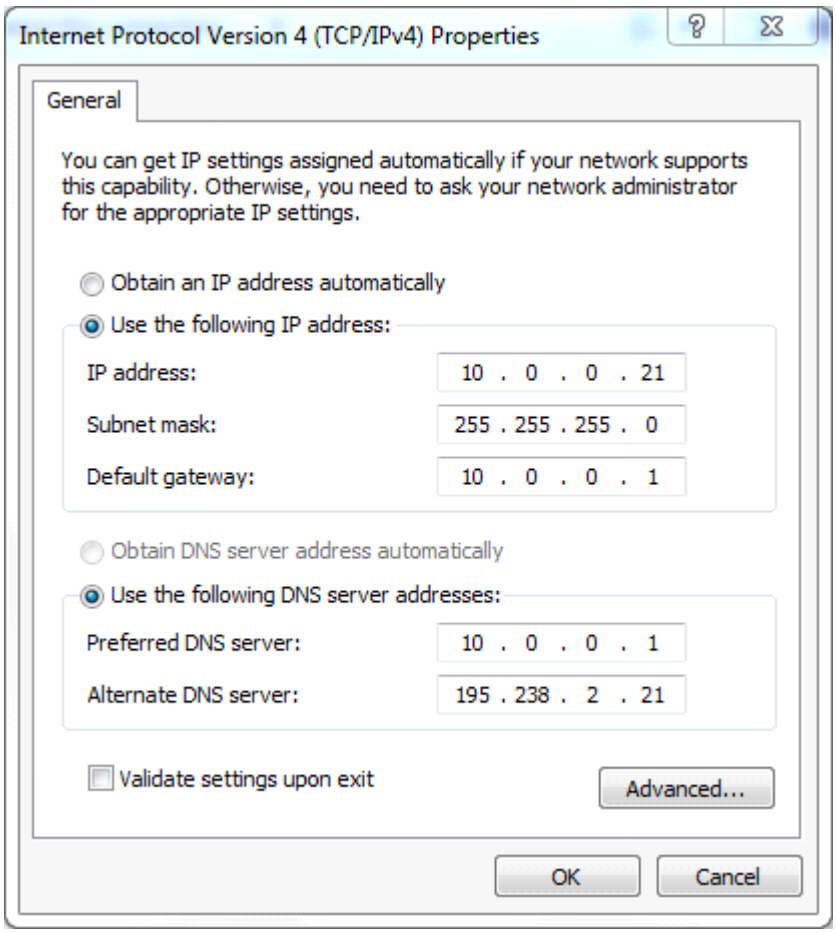
Click **Change adapter settings**.



Right click on **Local Area Connection** and select **Properties**.



Select *Internet Protocol Version 4 (TCP/IPv4)* and click ‘Properties’.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 21
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 1
Alternate DNS server: 195 . 238 . 2 . 21
Validate settings upon exit
Advanced...
OK
Cancel

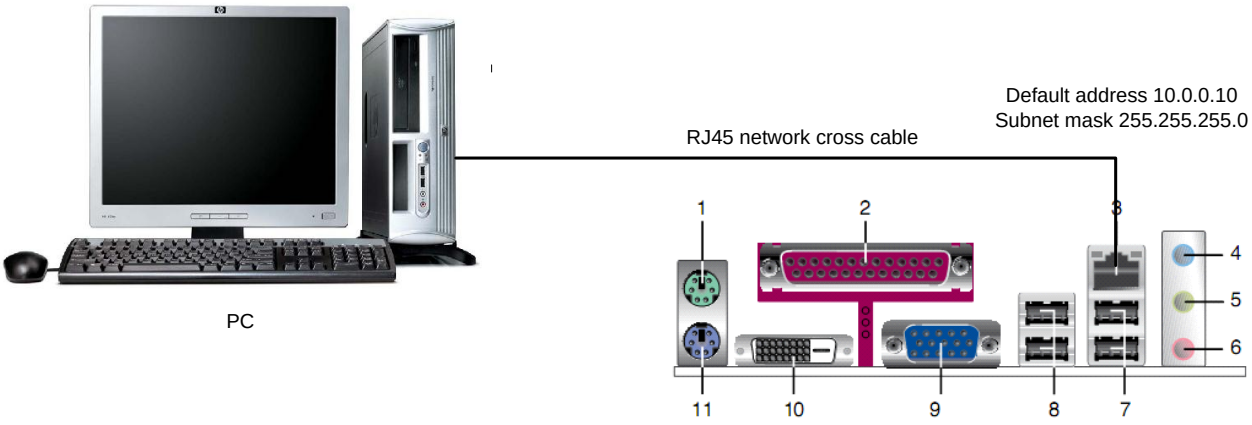
For ease of initial setup, you should change the PC's TCP/IP settings to the following:

IP address	10.0.0.2
Subnet mask	255.255.255.0

Click 'OK' to return to the Local Area Connection panel. Again click 'OK' to close this panel.

3.3 Installing the FastTrace 2 Client Software

Connect your PC to the FastTrace 2 video system with an RF45 network cross cable or through the network switch / router.

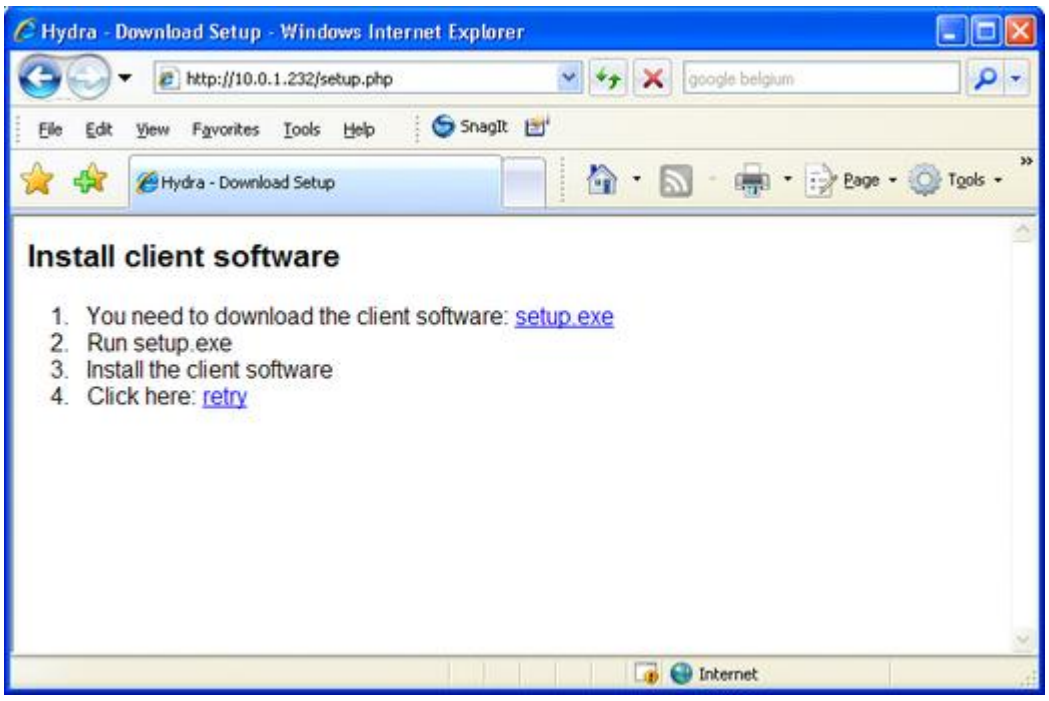


PC

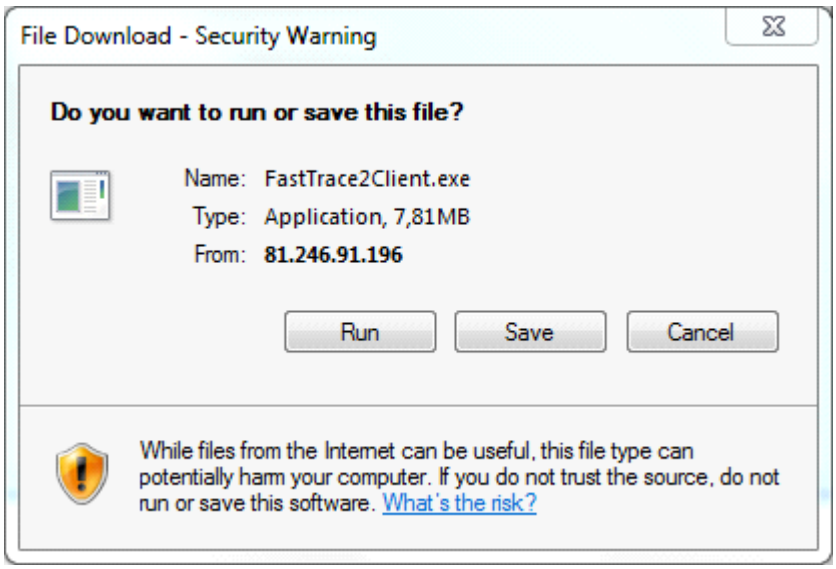
FastTrace 2

Open Internet Explorer and type the address of the FastTrace 2 video system in the address bar. If necessary add the setup page to the address: http://10.0.0.10/setup.php.

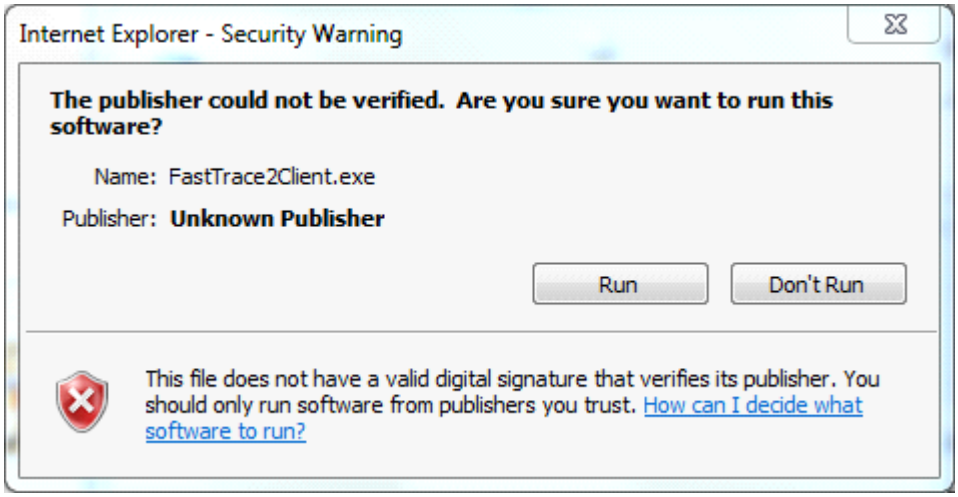
If you don't know the IP address of the FastTrace 2, see Retrieving the IP address of the FastTrace 2 .



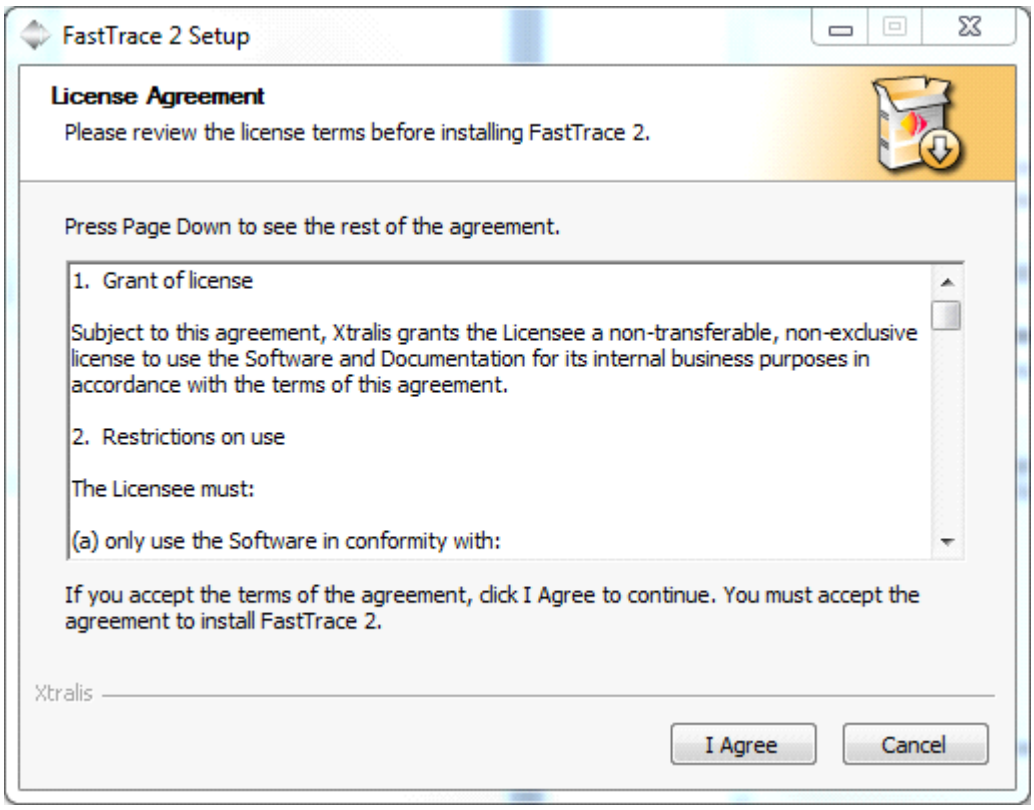
Click **setup.exe**.


File Download - Security Warning
Do you want to run or save this file?
Name: FastTrace2Client.exe
Type: Application, 7,81MB
From: 81.246.91.196
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

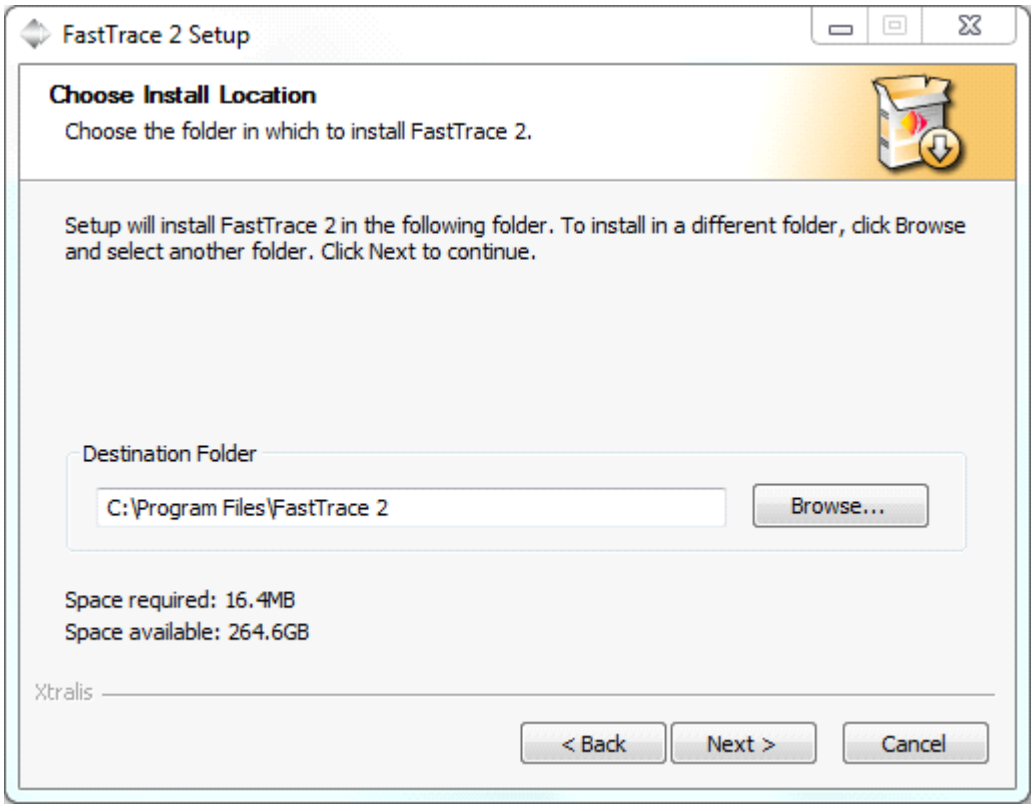
Click ‘Run’ to start the installation. You can also click ‘Save’ to store the file on your PC so that you can run the installation later.


Internet Explorer - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: FastTrace2Client.exe
Publisher: Unknown Publisher
Run
Don't Run
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

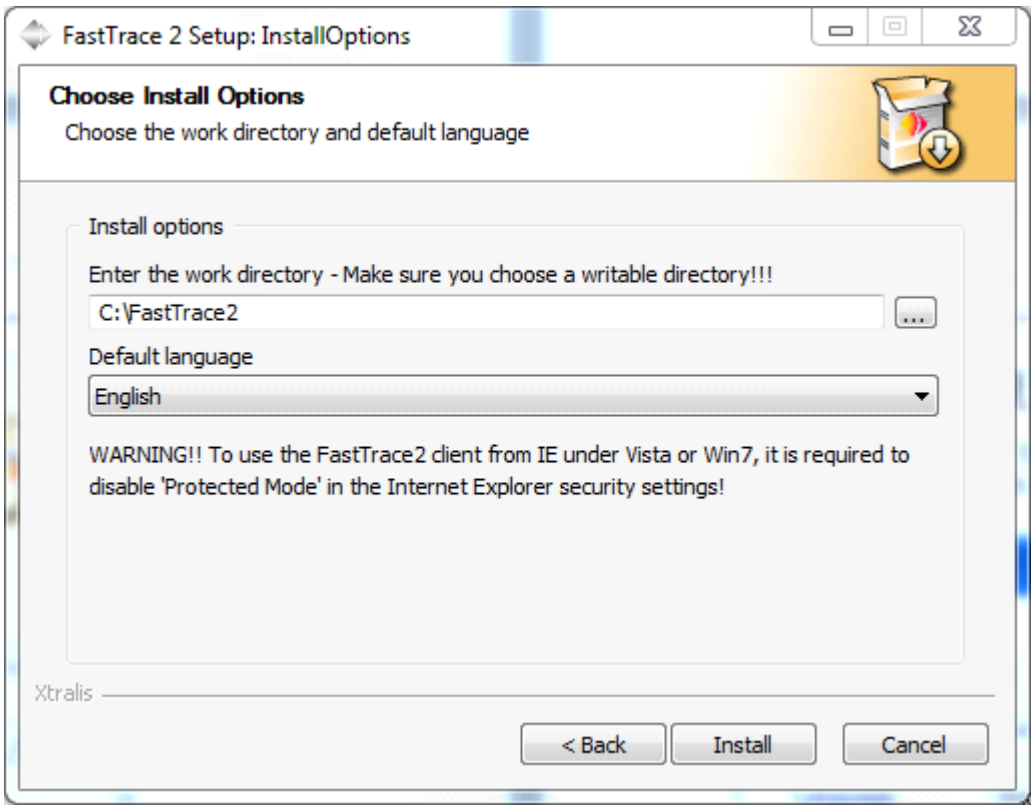
If you get the message above, click ‘Run’.


FastTrace 2 Setup
License Agreement
Please review the license terms before installing FastTrace 2.
Press Page Down to see the rest of the agreement.
1. Grant of license
Subject to this agreement, Xtralis grants the Licensee a non-transferable, non-exclusive license to use the Software and Documentation for its internal business purposes in accordance with the terms of this agreement.
2. Restrictions on use
The Licensee must:
(a) only use the Software in conformity with:
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install FastTrace 2.
Xtralis
I Agree
Cancel

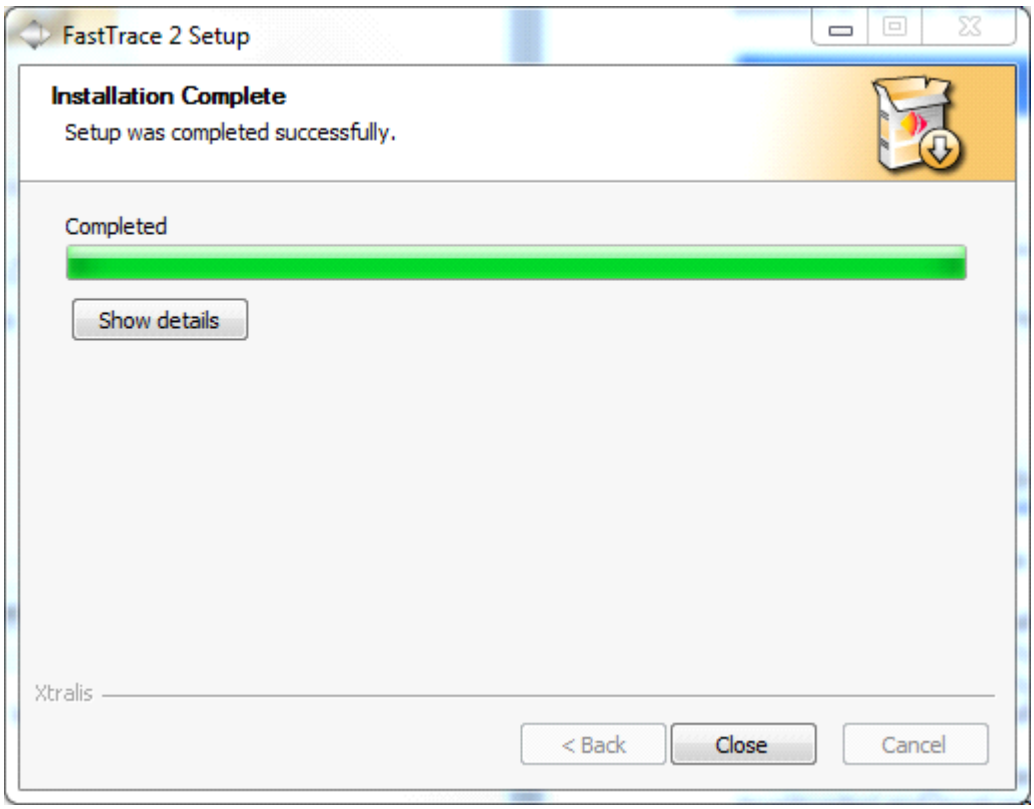
Click ‘Run’ to begin the installation of the Client software. When showing the License Agreement window, you need to agree with the terms. Click ‘I Agree’.


FastTrace 2 Setup
Choose Install Location
Choose the folder in which to install FastTrace 2.
Setup will install FastTrace 2 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\FastTrace 2
Browse...
Space required: 16.4MB
Space available: 264.6GB
Xtralis
< Back
Next >
Cancel

Accept or modify the installation folder. Click ‘Next’.


FastTrace 2 Setup: InstallOptions
Choose Install Options
Choose the work directory and default language
Install options
Enter the work directory - Make sure you choose a writable directory!!!
C:\FastTrace2
...
Default language
English
WARNING!! To use the FastTrace2 client from IE under Vista or Win7, it is required to disable 'Protected Mode' in the Internet Explorer security settings!
Xtralis
< Back
Install
Cancel

Accept or modify the work folder. Also select your preferred language. Click ‘Install’.



The installation is now completed. Click ‘Close’ to exit this installation wizard.

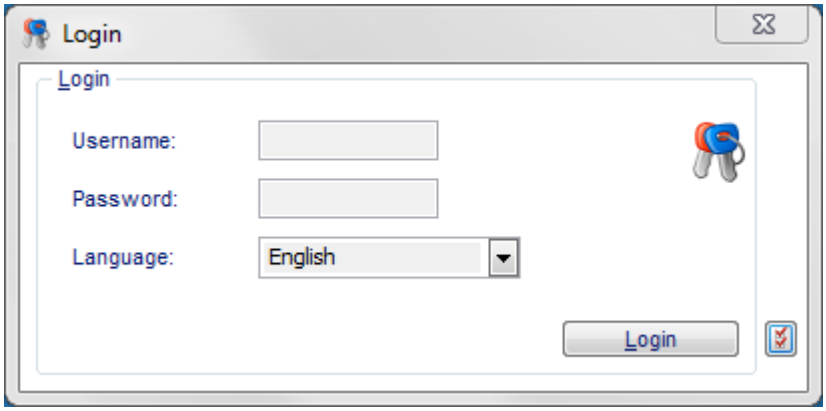
Remark:

The FastTrace 2 Client version 2.06.xxxx is compatible with the V3100 Hybrid (version 2.01.xxxx) and all previous V3100 server versions. However, some configuration menus, like “Video” and “Recording behaviour”, may look different, depending on the video system you are setting up and the licenses that have been installed.

3.4 Initial configuration

3.4.1 Launching the FastTrace 2 client in Internet Explorer

Open Internet Explorer. Type the IP address of the FastTrace 2 in the address bar (by default the IP address is 10.0.0.10 with subnet mask 255.255.255.0).



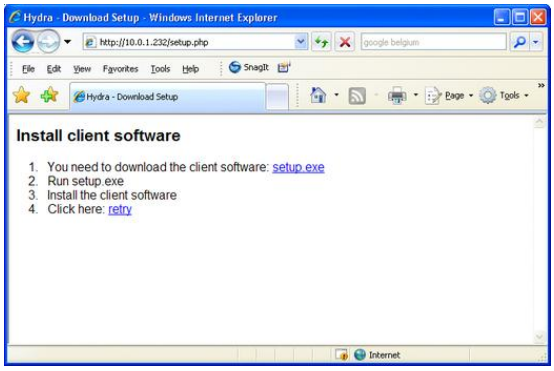
Provide a valid username and password.

3 users are by default validated in the FastTrace 2:
- User “0” with default password “666777”
- User “1” with default password “666777”
- User “15” with default password “666777” (= technician)

If required, change the language and check whether your work folder (= the folder in which downloaded and local recordings are stored) is correct.

Click *when you can’t see the work folder path!*

Click ‘Login’.


Hydra - Download Setup - Windows Internet Explorer
Install client software
1. You need to download the client software: setup.exe
2. Run setup.exe
3. Install the client software
4. Click here: retry

Mind:

It might occur that – even after the Client has been installed - the internet browser is opened instead of the login screen. If this is the case, just click “Retry”.

3.4.2 Launching the FastTrace 2 client in its own window

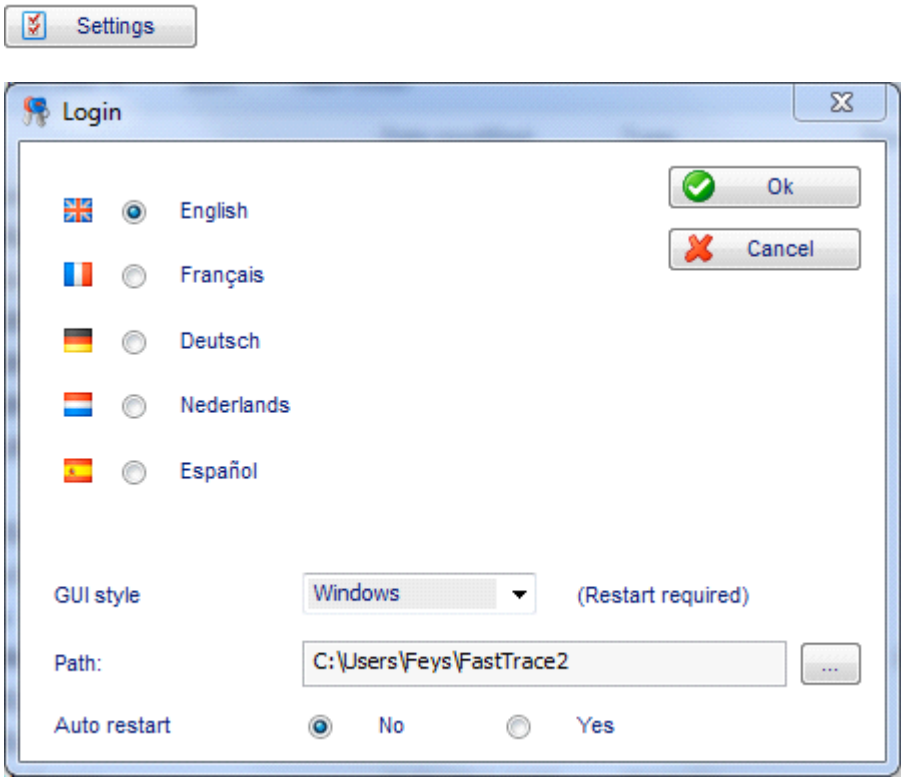
On the desktop, double click the FastTrace 2 shortcut:

You will get a login window:

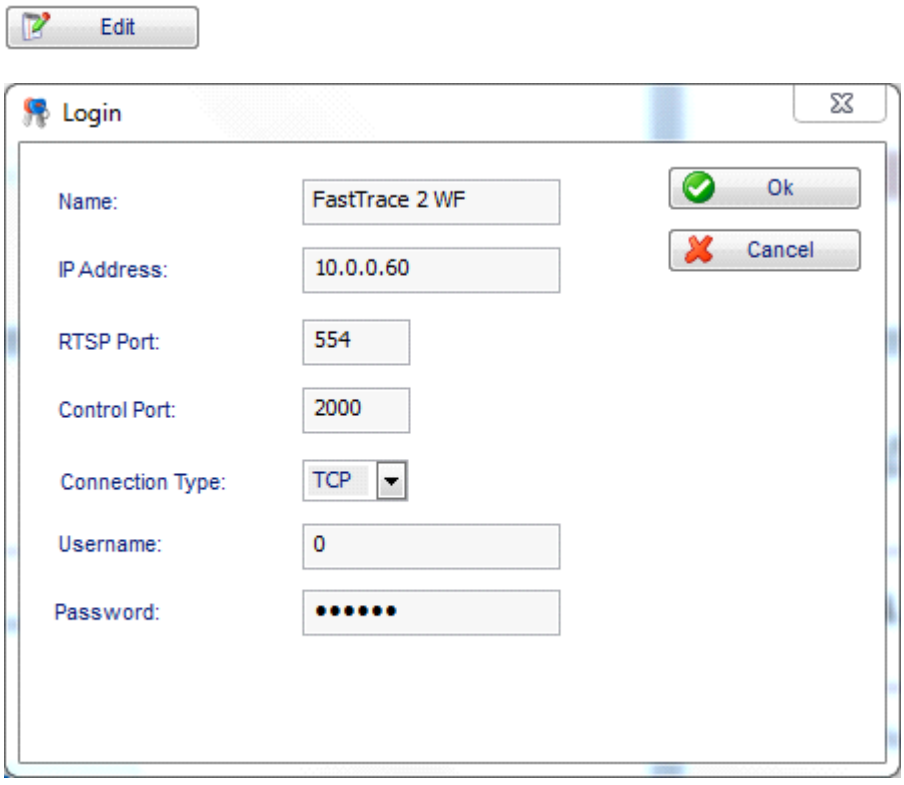
Select the desired video system from the list and click **Connect**.

When using the FastTrace 2 Client for the first time, you need to add a FastTrace 2 server first.
(see Adding a FastTrace 2 server to the FastTrace 2 client)

Via **Settings** you can change the language, the skin (= appearance of the program), the work folder (in which downloaded and local recordings are stored) and the auto restart settings:

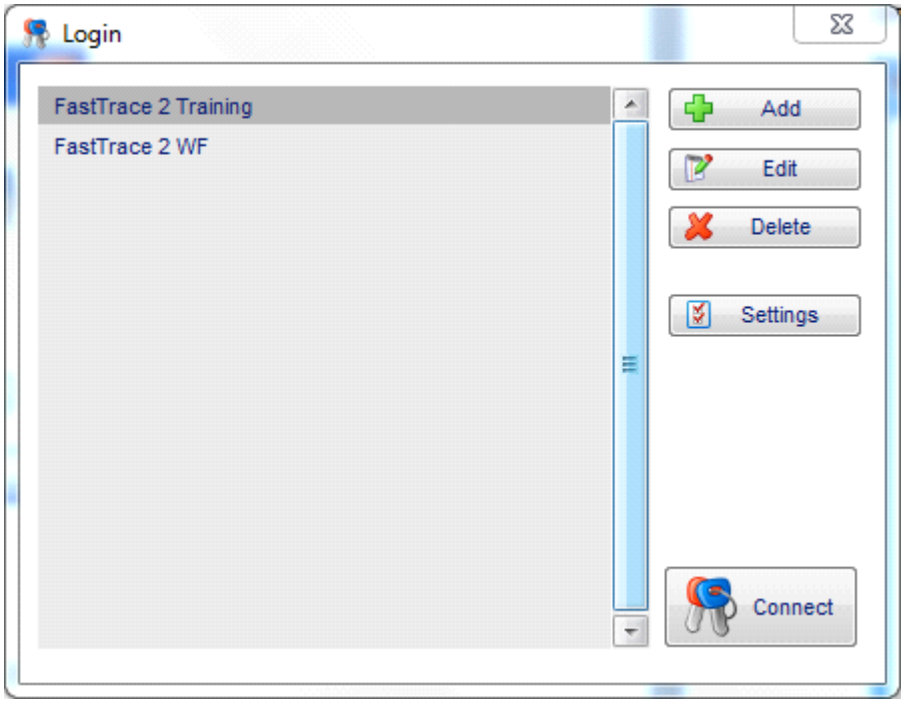


Via **Edit** you can modify necessary ports or change user (with valid password). It is also recommended to provide a useful and meaningful name for your video system.



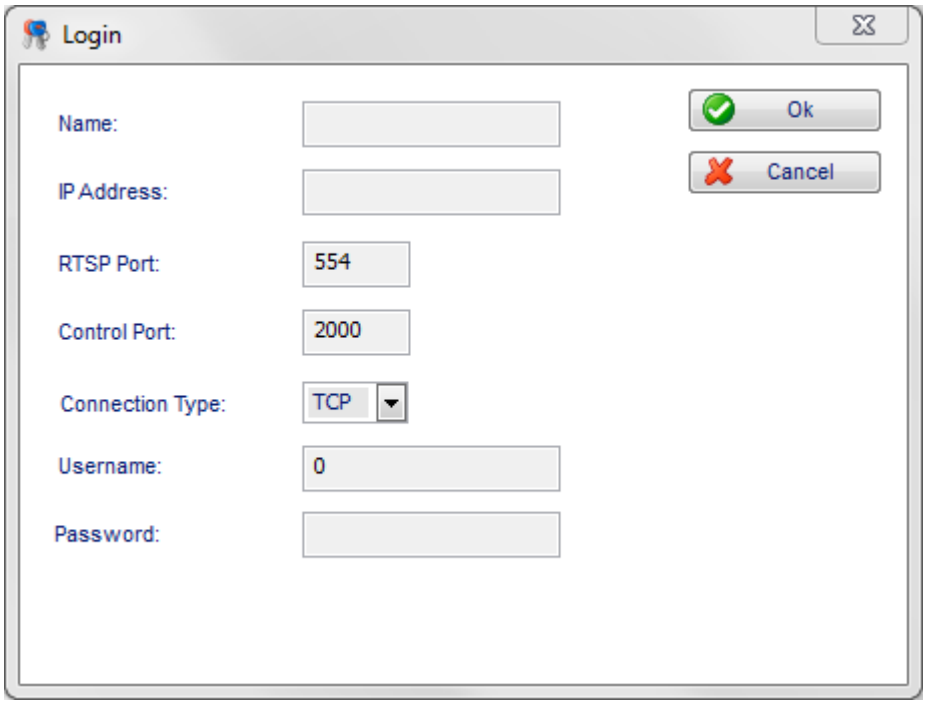
3.4.3 Adding a FastTrace 2 server to the FastTrace 2 client

Launch the FastTrace 2 client (in its own window).



Click **Add**.

You will get this window:



Please fill in all necessary information.

- Enter a description as “Name”. It is recommended to provide a meaningful description to your FastTrace 2 video system!
- Enter the IP address of the FastTrace 2 (by default 10.0.0.10).
- Set RTSP port and Control port. Use the same ports as specified under System > Ethernet/PPP (*see*).
- Select the TCP or UDP protocol. UDP is recommended, but TCP may be required if the connection goes through a router that blocks the UDP packets.
- Enter the username and password of an existing user. By default you can log on with user “0” and password “666777”.

Click **OK** to save the added device.

At this time you can select the newly added video system from the list and connect to it.

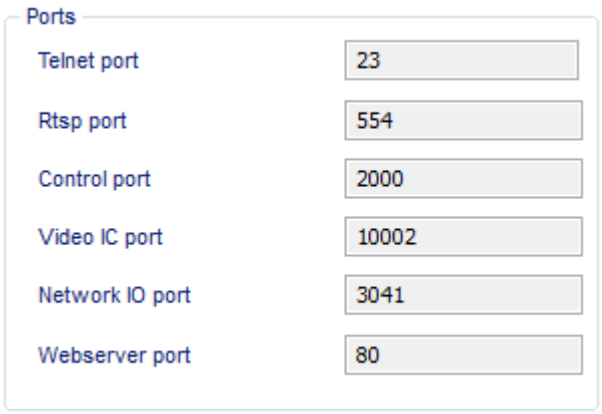
3.4.4 Network connections

The FastTrace 2 video system can be connected to a local network or to a remote (PPP dial-in) network, applying an external modem.

To set up the network connections, open **System > Connections > Ethernet/PPP**. Modify the settings and click **Save**.

3.4.4.1 Ports

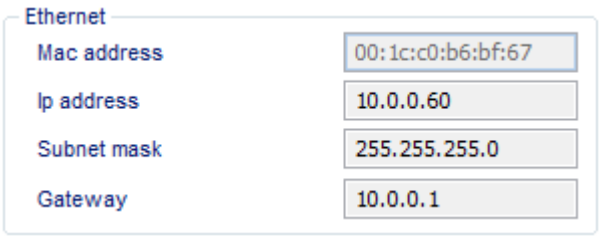
In this section you can set the ports that will be used.



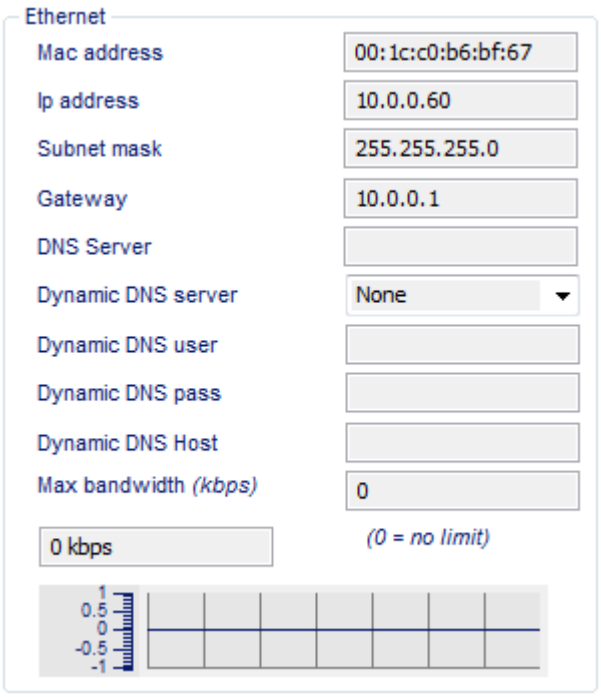
Port	Description	Default value
Telnet port	The IP port used to make a Telnet connection.	23
Rtsp port	Real time streaming protocol: this port is used by the FastTrace 2 Client to control the video streaming. *You have to use the same value here as the value specified when adding this video system in the FastTrace 2 Client!* *(see Adding a FastTrace 2 server to the FastTrace 2 client)*	554
Control port	IP port used to exchange information between the FastTrace 2 video system and the FastTrace 2 Client software. (e.g. display status of inputs and outputs) *You have to use the same value here as the value specified when adding this video system in the FastTrace 2 Client!* *(see Adding a FastTrace 2 server to the FastTrace 2 client)*	2000
Video IC port	Port used to interconnect with S3100 security panels. This allows starting a recording on an alarm detected on the security panel. *Use the same port as the one selected in the S3100 configurator!*	10002
Network IO port	Port used to poll the Net I/O modules.	3041
Webserver port	Port used for the http protocol.	80

3.4.4.2 Ethernet connection

Enter all necessary information for the Ethernet connection in this section.



Click on Advanced mode to define the DNS settings.



Parameter	Description	Default value
Mac address	Shows the Mac address of your video system.	-
IP address	Enter the IP address of the FastTrace 2 video system. Do not use reserved addresses!	10.0.0.10
Subnet mask	Enter the subnet mask.	255.255.255.0
Gateway	Set the gateway (= IP address of the router).	10.0.0.1
Provider DNS Server	Enter the provider DNS server. The FastTrace 2 needs this information to be able to connect to the Dynamic DNS Server. When using internet over Ethernet this field is optional, because certain protocols have been programmed in the software, when the internet connection is only available via a 3G modem (in the PPP section), this field is obligatory.	-
Dynamic DNS server	Choose the correct provider from the list. **Mind:** first the Dynamic DNS account (with any Dynamic DNS service provider) needs to be set up!	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	-

Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	-
Dynamic DNS host	Enter the host you have received from your provider for your Dynamic DNS account.	-
Max. bandwidth	This limits the total bandwidth used by the video system. This may affect image rate, but not the image quality, during live viewing. The value is expressed in kbps.	0 (no limit)
Currently used bandwidth	This shows the current bandwidth usage, both the value and the graphical view. The value is expressed in kbps.	-

3.4.4.2.1 Configuring Dynamic DNS settings

Enter the required parameters – either in the Ethernet or the PPP section – and click **Save**. Wait about 10 seconds. If an error occurs during the connection to the Dynamic DSN service, an error window will pop up. At the same time an alarm will be set. This alarm can be viewed in the Status window. Faults can be due to a faulty login, wrong password or wrong host name.

To register to a Dynamic DNS service provider, the FastTrace 2 needs access to the internet and to a DNS server to resolve the host name of the service provider. This internet connection can be provided by the Ethernet connection or a 3G connection. When the internet connection is only available through 3G, it is necessary to enter the correct Provider DNS server in the Ethernet section!

Mind:

If you configure a Dynamic DNS service for both the Ethernet and the PPP (3G) connection, it is necessary to use different host names!

Note:

When the FastTrace 2 is behind a router, the external IP address will be used by the Dynamic DNS service. This will automatically be set by the FastTrace 2, so no changes in the FastTrace 2 settings are necessary!

3.4.4.2.2 Dynamic DNS error messages

3.4.4.2.2.1 Warning: Unable to determine IP address

If you receive this error message, the FastTrace 2 could not resolve the service provider's host name. Please check the DNS server in the Ethernet section or check the internet connection of the FastTrace 2.

3.4.4.2.2.2 No update required

When changing settings to the Dynamic DNS section in the FastTrace 2, the video system will write a new configuration and force an update of this configuration. Some service providers are not very happy with this procedure and might return a message like "No update required" or "Attempts to change to the current address are considered abusive". This alarm will automatically reset on the next automated check after one minute.

Note:

An error message is displayed only once. If you want to review the message once again, set the Dynamic DNS Server to *None*, click **Save**, then re-enter your DNS provider and click **Save** again. Wait a few seconds and the message will reappear.

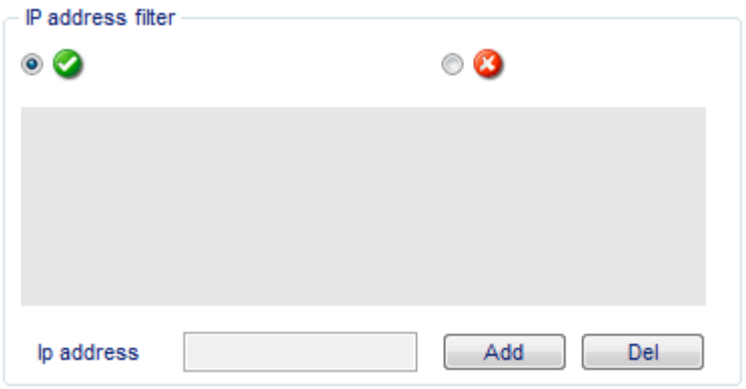
3.4.4.2.3 What's the use of using Dynamic DNS?

Dynamic DNS provides the capability for a networked device, such as a router or modem, to notify a Domain Name System (DNS) to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information. Thus a hostname can be used instead of the IP address, which is very interesting for DHCP attributed IP addresses. Especially with 3G the IP address is often attributed by DHCP.

It also becomes possible to automatically update the Client software.

3.4.4.3 Granting access to the FastTrace 2 video system

To limit the access to the video system, you can either enter a list of authorized clients (the *green* option) or a list of non-authorized clients (the *red* option). Your choice of course depends on the specific situation. This is only displayed in the *Advanced mode*!



Click **Add** to add an IP address to the selected list.

Mind:

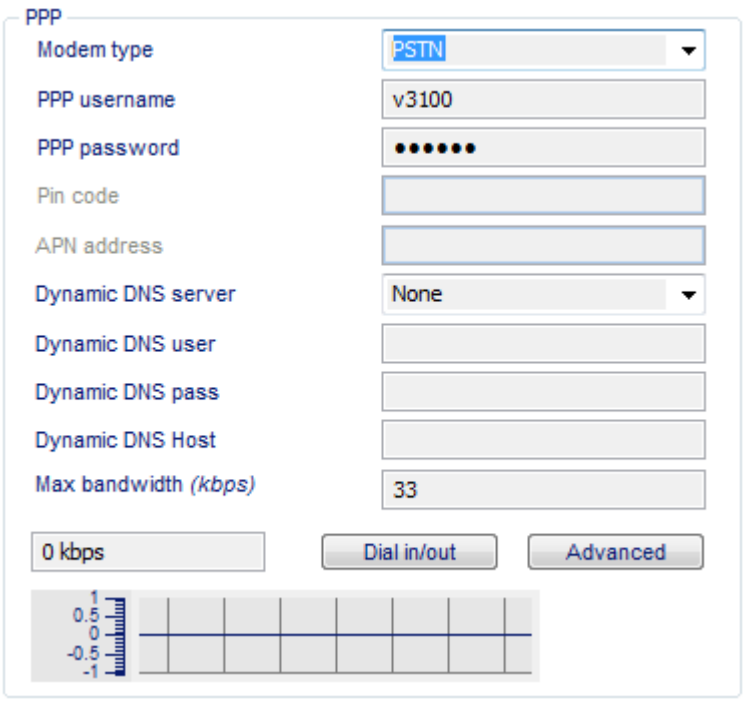
You **cannot** use both lists at the same time!

3.4.4.4 PPP connection

You need to access the *Advanced mode* to be able to configure the PPP settings!

3.4.4.4.1 PSTN or ISDN modem Configuration

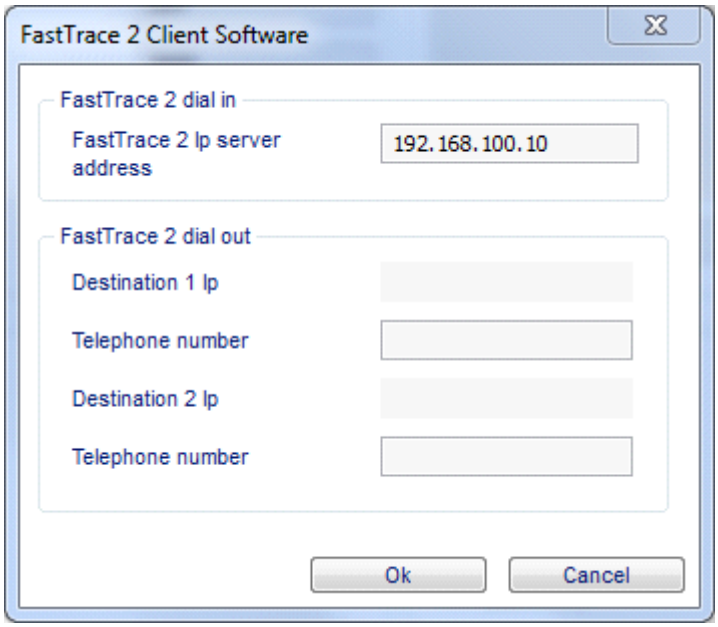
When a PSTN or ISDN modem is connected to the FastTrace 2 video system, choose the option *PSTN* for modem type in the *PPP* section.



Parameter	Description	Default value
Modem type	Set the modem type to PSTN when using a standard modem that uses the analogue line (AT modem) or digital line (ISDN). The modem should always be connected to the first USB port /dev/ttyU1. (*see Required motherboard*)	None
PPP username	The login username of a user allowed to connect to the dial-in network (PPP authentication).	V3100
PPP password	The login password of a user allowed to connect to the dial-in network (PPP authentication).	666777
Dynamic DNS server	Choose the correct provider from the list. **Mind:** first the Dynamic DSN account (with any Dynamic DNS service provider) needs to be set up!	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	-
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	-
Dynamic DNS Host	Enter the host you have received from your provider for your Dynamic DNS account.	-
Max bandwidth	This limits the bandwidth used by the video system. This may affect image rate, but not image quality, during live viewing. The value is expressed in kbps. “0” means no limit.	33 *(suitable for V34 modem)*
Currently used	This shows the current bandwidth usage, both the value and	-

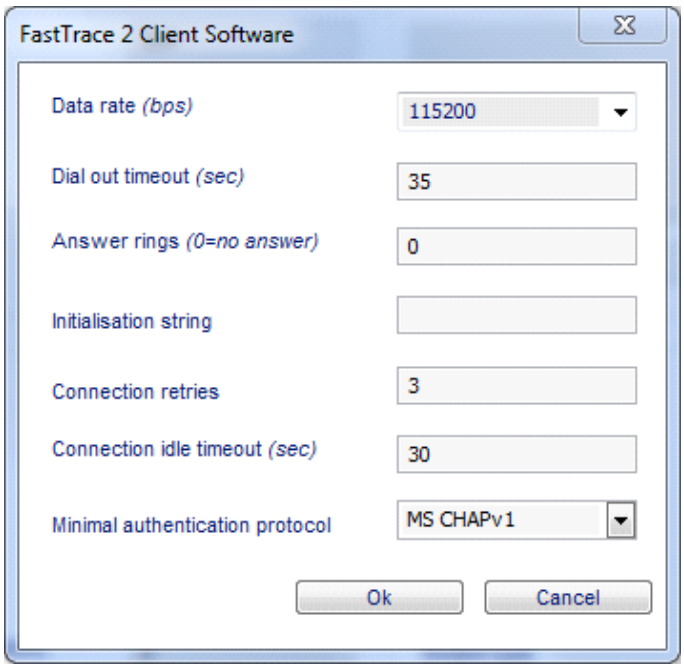
bandwidth	the graphical view. The value is expressed in kbps.	

Click **Dial in/out** to open this window:



Parameter	Description	Default value
IP address FastTrace 2 server	This is the IP address that will be assigned to the FastTrace 2 video system when a remote connection has been established by the client.	192.168.10.10
Destination 1 IP	The IP address of the computer to which alarms have to be sent.	-
Telephone number	The number to dial to connect to the monitoring site.	-
Destination 2 IP	The IP address of the computer to which alarms have to be sent, in case the first IP address is not responsive.	-
Telephone number	The number to dial to connect to the monitoring site when the first telephone number is not responsive.	-

Click **Advanced** to open this window:



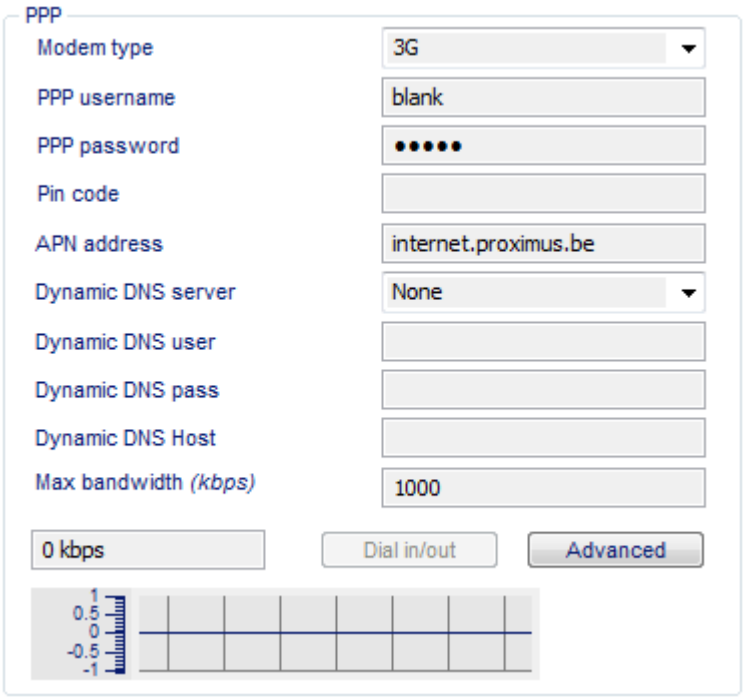
Parameter	Description	Default value
Data rate (bps)	This sets the baudrate of the modem.	115200
Dial out timeout (sec)	This sets the time in which a connection has to be established with the remote client. If not successful, the video system will retry to make the connection. The number of attempts is limited by the parameter “Connection retries”. Be aware that a PPP connection over PSTN can easily take 30 to 60 seconds.	35
Answer rings (0=no answer)	This sets the number of rings on an incoming call before hooking off.	0 (*do not answer any call*)
Initialisation string	Hayes command string to initialize the modem.	-
Connection retries	The number of attempts the video system will make to connect to the remote client.	3
Connection idle timeout (sec)	This sets the delay after which the video system will disconnect if no more data is exchanged.	30
Minimal authentication protocol	Selects the authentication protocol that will be used during the setup of a remote connection: PAP/CHAP/MSCHAPv1/MSCHAPv2.	MS CHAPv1

See also Alarms.

3.4.4.4.2 3G modem Configuration

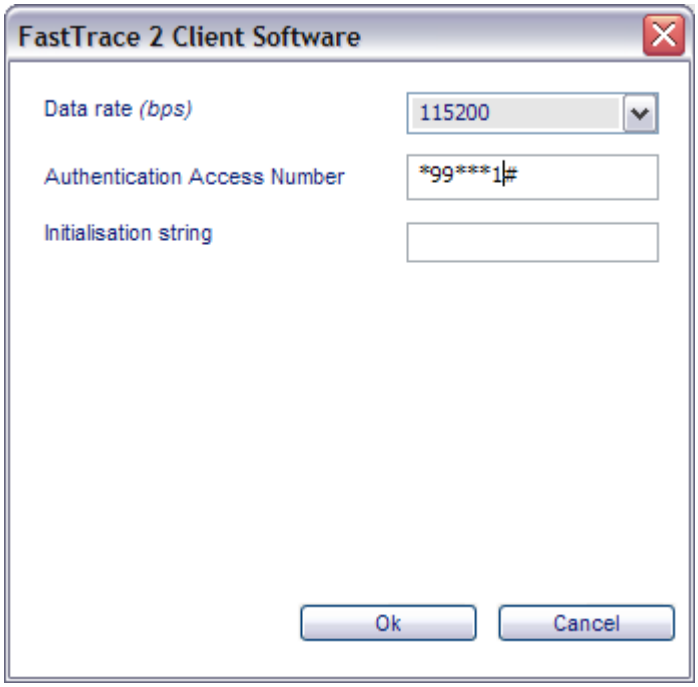
When a 3G modem is connected to the FastTrace 2 video system, choose the option *3G* for modem type in the *PPP* section.

Mind: only the Wavecom FastTrack extend 3G modem (now obsolete) and the Sierra Wireless Airlink Raven XE modem can be supported by the FastTrace 2. There's no guarantee that any other 3G modem will work properly.



Parameter	Description	Default value
Modem type	Set the modem type to 3G when using a 3G modem.	None
PPP username	The login username of a user allowed to connect to the dial-in network (PPP authentication).	blank
PPP password	The login password of a user allowed to connect to the dial-in network (PPP authentication).	blank
Pin code	Enter the pin code for your 3G SIM card.	-
APN address	Enter the APN (Access Point Name) address of your provider.	-
Dynamic DNS server	Choose the correct provider from the list. **Mind:** first the Dynamic DSN account (with any Dynamic DNS service provider) needs to be set up!	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	-
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	-
Dynamic DNS Host	Enter the host you have received from your provider for your Dynamic DNS account.	-
Max bandwidth	This limits the bandwidth used by the video system. This may affect image rate, but not image quality, during live viewing. The value is expressed in kbps. "0" means no limit.	1000
Currently used bandwidth	This shows the current bandwidth usage, both the value and the graphical view. The value is expressed in kbps.	-

Click ‘Advanced’ to open this window:



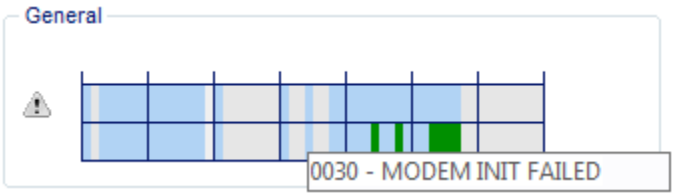
Parameter	Description	Default value
Data rate (bps)	This sets the baudrate of the modem.	115200
Authentication Access Number	This number will be dialled by the 3G modem to setup a data connection. The number depends on the country and/or the provider. E.g.: Vodafone in Australia uses *99***2#.	*99***1#
Initialisation string	Hayes command string to initialize the modem.	

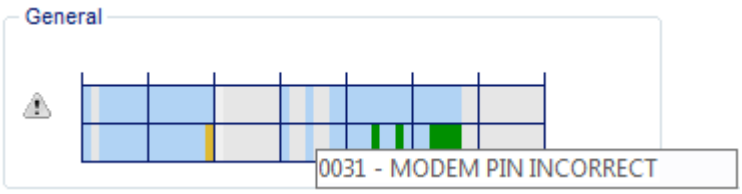
See also Alarms.

Note:

The moment you choose 3G as modem type, and save, the FastTrace 2 video system will automatically search for the internal 3G connection.

To display the progress the error “Modem init failed” appears on the Status page. This error message should disappear after about 45 seconds (depending on the connection) upon establishment of the 3G connection. If the error message doesn’t disappear, there is a problem with the modem USB connection or the 3G settings. When you have entered an incorrect pin code the error message “Modem pin incorrect” will appear.





When a 3G connection is setup successfully, but no connection can be made, try changing the port on the Ethernet page. The default control port is 2000, but that port is blocked by most providers. Changing the port to port 2001 should resolve the problem.

4 Using IP cameras

4.1 Technical specifications

Maximum number of cameras	16 (total of analogue and IP cameras)
IP cameras (*)	up to 16 IP cameras on a dedicated IP network; optional network interface (HIPI card) required; 1 HIPI card per 8 IP cameras; only H264 video streaming can be used; audio input is supported
Video output	VGA connector; adjustable resolution (up to SXGA)
Video compression	H.264
Audio compression	The audio compression depends on the camera type.
IP cameras video resolution and images/second	Depends solely on the IP camera type. Maximal HD resolution.
Bandwidth	Remotely adjustable: compression, ips and quality. A bandwidth limit can be specified.
Recording type	Continuous, on event (e.g. input, motion detection), alarm over IP (S3100)
Remote visualisation	Internet Explorer; Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008
PTZ cameras	Several protocols available (*see also* List of available PTZ protocols)
Management	- Internet Explorer (installs Client software) - VSKwin software - M3000 software - 3rd party CMS software

(*) *With an ENTRY system license you cannot use IP cameras, because this is not supported by this specific system license! This is for instance the case with the ADPRO FastTrace 2 Lite.*

Important:

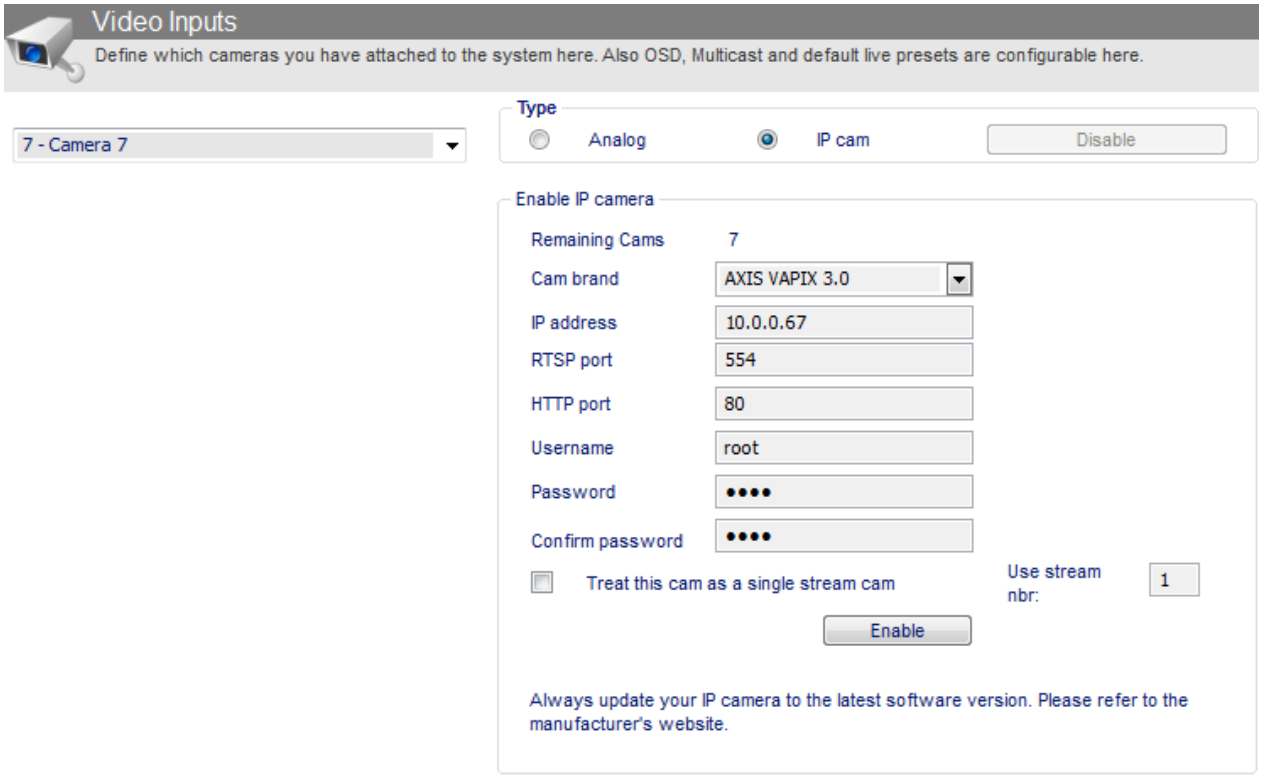
No other streams may be drawn from the IP camera than those destined for the FastTrace 2! If you do need to draw streams from the IP camera for any other reason, please use the single stream mode (see Video streams).

If you have to use streams for other applications as well, please use the single stream mode then.

4.2 IP camera setup

IP cameras can be connected to the HIPI card or to the main network. 1 HIPI card is required per 8 cameras.

To add an IP camera, you need to connect the camera to the network and open **System > Connections > Video inputs**. Then choose a free camera number from the drop down list:

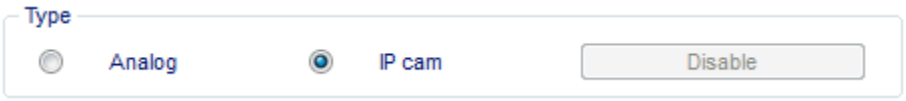


Up to 16 cameras can be connected to the FastTrace 2 video system. Up to 8 cameras 1 HIPI card is sufficient; from up to 9 cameras you will need a second HIPI card.

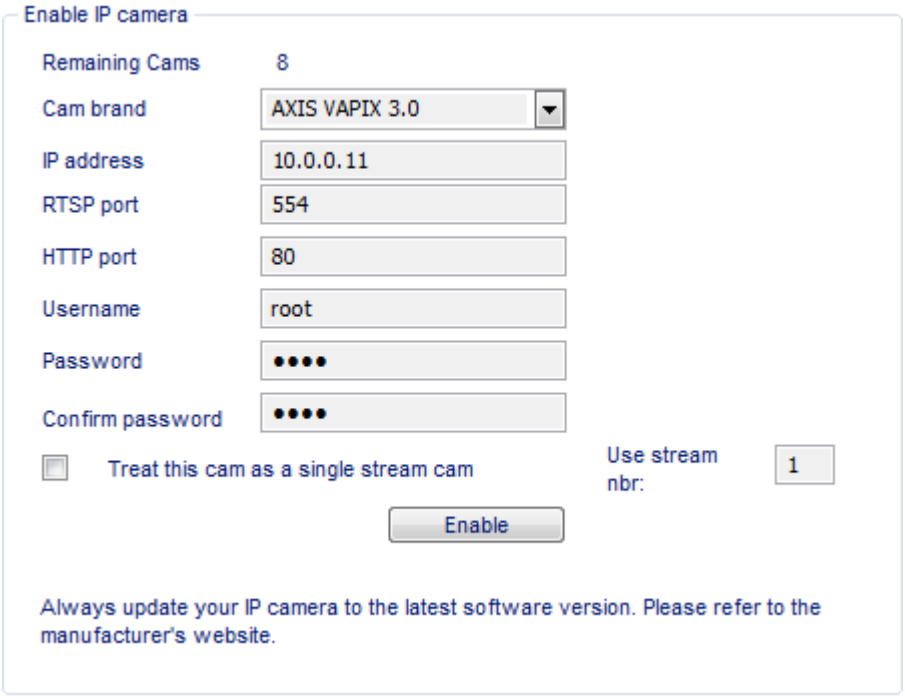
Mind:

You need to configure the HIPI card(s) before configuring the IP cameras.
(see Update and configure the HIPI card*)*

Tick the IP cam option:



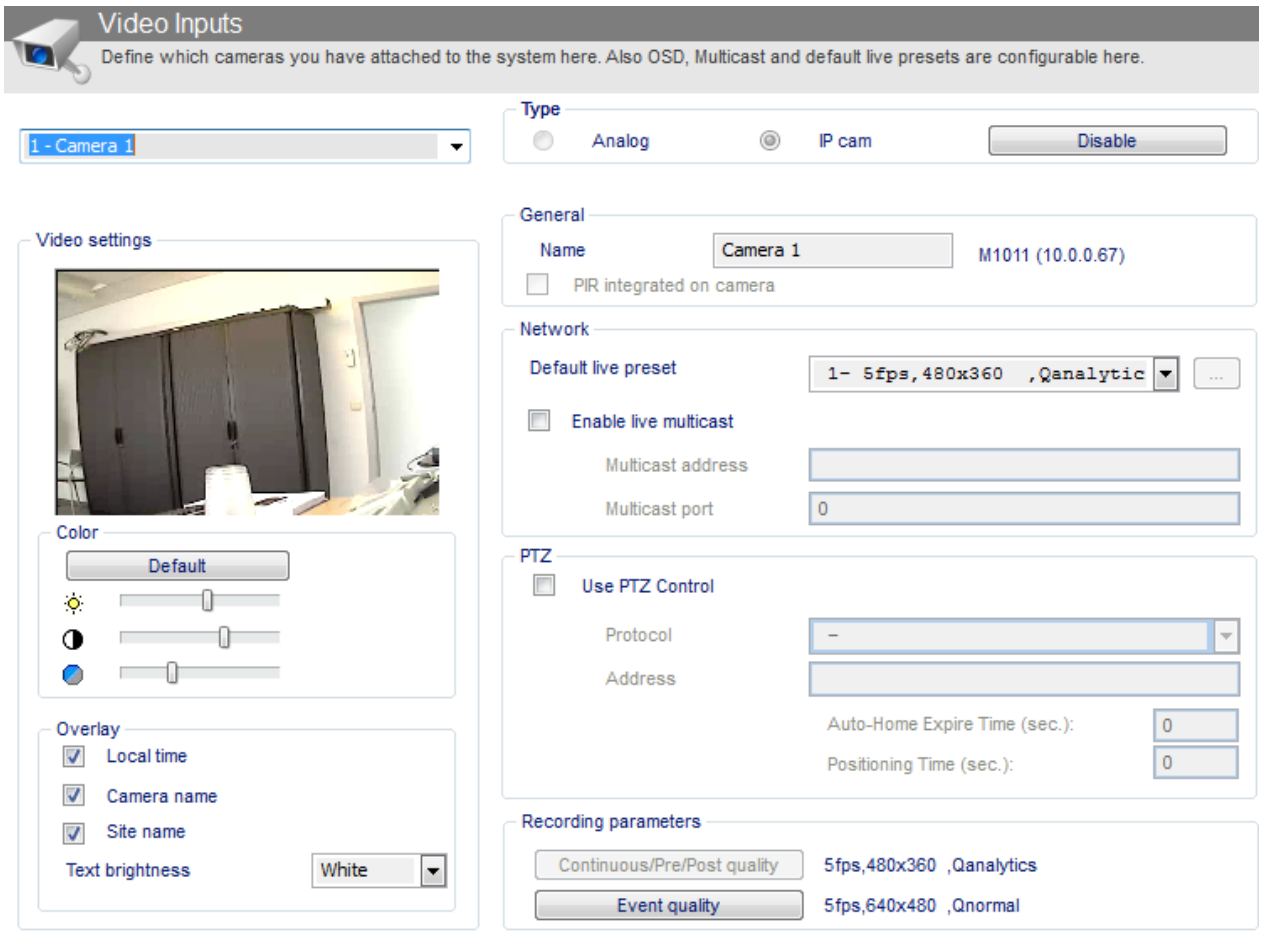
Select the camera brand and enter the correct IP address, the username and corresponding password of the camera (e.g. “root” for Axis cameras). Check the camera documentation for this password!



If you tick the option *Treat this cam as a single stream cam*, only one stream will be used for all features related to the FastTrace 2 server. This means, however, that there will be specific limitations in the FastTrace 2 video system: the only stream that the FastTrace 2 video system will use is the analytics stream. As a result this will be a CIF resolution at 5 fps (or the minimal quality available on the camera).

(see Video streams)

Click ‘Enable’ to start using the IP camera.



Then complete the necessary parameters.

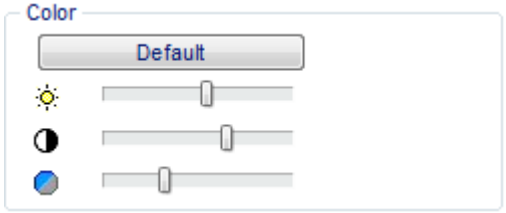
4.2.1 General parameters

Name	Enter a description for the camera (max 20 characters). *It is recommended to use a meaningful and relevant description.*
PIR integrated on camera	Check this option when a PIR has been integrated on this camera.

4.2.2 Video settings

4.2.2.1 Color

If the image does not provide enough quality, you can adjust brightness, contrast and hue in the “Color” section.



4.2.2.2 Overlay

Local time	Tick this option if you want to visualize the local time on the camera's live image.
Camera name	Tick this option if you want to visualize the camera name on the camera's live image.
Text brightness	This option is not available for IP cameras. The parameter can be added to the IP camera settings via the camera's web browser.
Site name	Tick this option if you want to visualize the site name on the camera's live image.

4.2.3 Network

Default live preset	When watching live images from a camera, the image quality can be adjusted at any time by clicking your right mouse button. The initial quality, applied the first time you select the camera, can be specified with this parameter. You can choose from different preset qualities, depending on the camera. If you choose "Hard disk stream", live pictures will follow the same quality as continuous recordings. This way, only two streams are required.
	With certain types of IP cameras this button becomes active. Via this button you can open the list with possible quality presets. The parameters you can modify here, are: - Frames per second (fps) - Resolution of the picture - Quality: VBR quality (Qlow, Qnormal or Qhigh) or CBR bit rate (20 through 2048 kbps). The higher the value, the better the quality, but also the higher the bandwidth use! *Remark: for stable image quality VBR is recommended.*
Only live multicast	Multicast is the simultaneous supply of information to one or more computers through only one data stream from the source. When multiple computers poll this one stream, multiple copies will be created, but the initial upload will remain the same. Multicast thus ensures less data traffic over the network. The 224.0.0.0 through 239.255.255.255 address range has been assigned for multicasting on the local LAN network. Tick this option if you want to use the multicast protocol.
Multicast address	Enter the address to which the FastTrace 2 video system has to send the multicast. ***Mind***: every camera should be assigned to a unique multicast address. Everyone who has subscribed to the multicast, can view the live images on this address, using a web browser or a FastTrace 2 Client.
Multicast port	Enter the multicast port through which the FastTrace 2 has to send the stream. ***Mind***: every camera should be assigned to a unique multicast port. This port must be defined by the IT Department before connecting the FastTrace 2.

4.2.4 PTZ

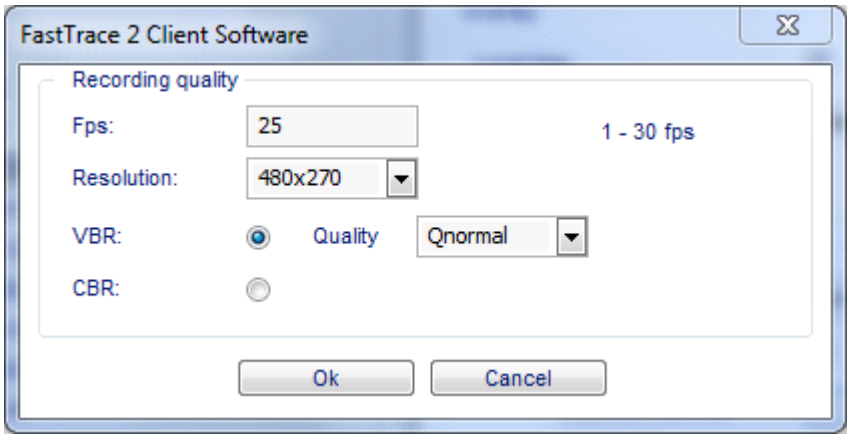
Use PTZ Control	Tick this option if you have installed a PTZ camera.
Protocol	Choose the corresponding protocol for the IP camera you have installed.
Address	Enter the correct camera address for the IP camera you have installed. Check the camera settings to know the camera address.
Auto-Home Expire	This value indicates the time in seconds that has to be expired after every PTZ

Time (sec)	action, before the PTZ camera will move back to its home position. If the value is left to 0, the Auto-Home feature will be disabled.
Positioning Time (sec.)	PTZ preset positions can be selected via an input. When that input triggers the PTZ action, the camera will move to the configured PTZ preset position, but the alarm message of the input will be delayed until the PTZ preset positioning time has expired. Thus no blurry images are recorded for quad images.

4.2.5 Recording

Continuous/Pre/Post quality	This shows the quality that has been configured for continuous recordings and for pre and post event recording.
Event quality	This shows the quality that has been configured for the event recording.

Set the recording parameters by clicking the desired quality.



- Fps: the number of frames (images) per second (1 – 25);
- Resolution: the number of pixels per image; depends on the camera type;
- VBR: selects a variable bitrate compression (Qlow, Qnormal or Qhigh);
  CBR: selects a compressed bitrate compression (value 20 – 2048 kbps); the higher the value, the higher the compression and the higher the loss of quality; the compression levels will differ according to the constant data flux in which the file size is predictable, but the quality will depend on the video contents.

VBR with Qnormal quality is recommended!

Click ‘Save’.

Remark:

Before using the IP camera, you need to set up a static IP address in the camera, create a password for the user “root” and set the date and time. You can adjust the time and date manually or you can synchronize the camera in the FastTrace 2 to an NTP protocol.

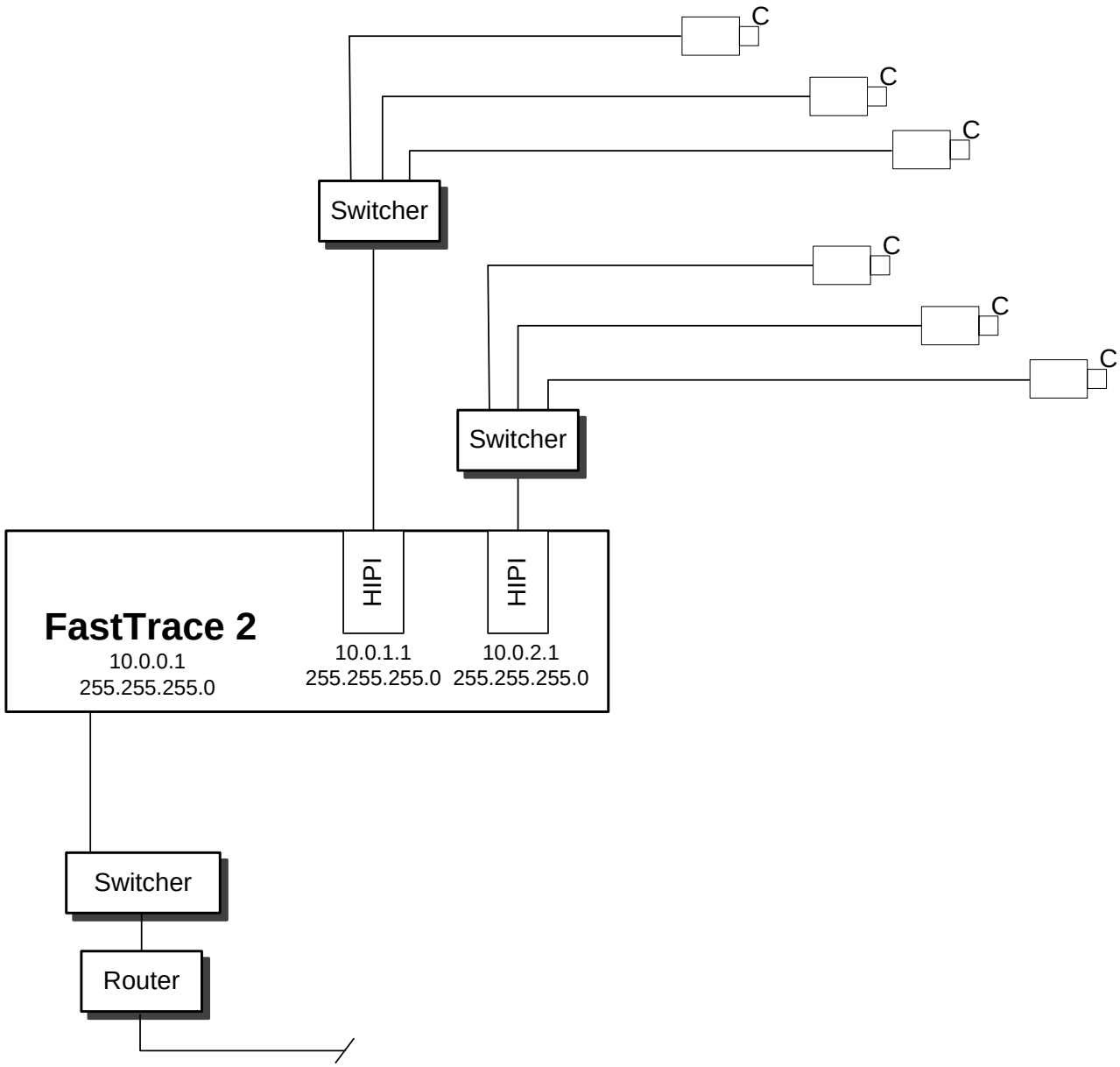
Check the manual provided with the camera for more information on setting up the IP address, password and clock.

4.3 Update and configure the HIPI card

The HIPI card offers an isolated LAN network (10/100/1000 Mbps on RJ54 connector) to connect IP cameras.

Important:
The Ethernet connection of your FastTrace 2 video system and the Ethernet connections of the installed HIPI cards must be set on different IP ranges! IP cameras can be connected on either HIPI card, as presented in the illustration underneath, with a maximum of 8 cameras per HIPI card. Yet, when two HIPI cards have been installed you can connect up to 16 IP camera's to the same Switcher / HIPI card.

Also mind that the HIPI Ethernet interfaces use ETH1 and/or ETH2, not ETH0!

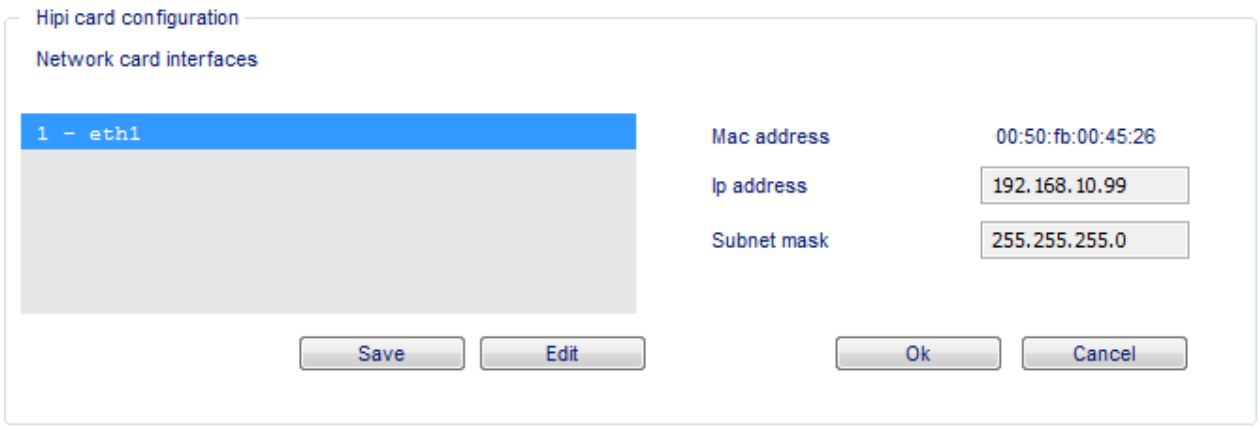


The HIPI card is automatically detected by the FastTrace 2 video system. Each HIPI card must be configured with a different IP address and a subnet mask. As a consequence, 3 IP ranges are possible on a FastTrace 2 configuration:

- IP range of the FastTrace 2 video system
- IP range of the first HIPI card
- IP range of the second HIPI card

All IP cameras connected to the HIPI card (by means of a switch) must be set in the same IP range as the HIPI card.

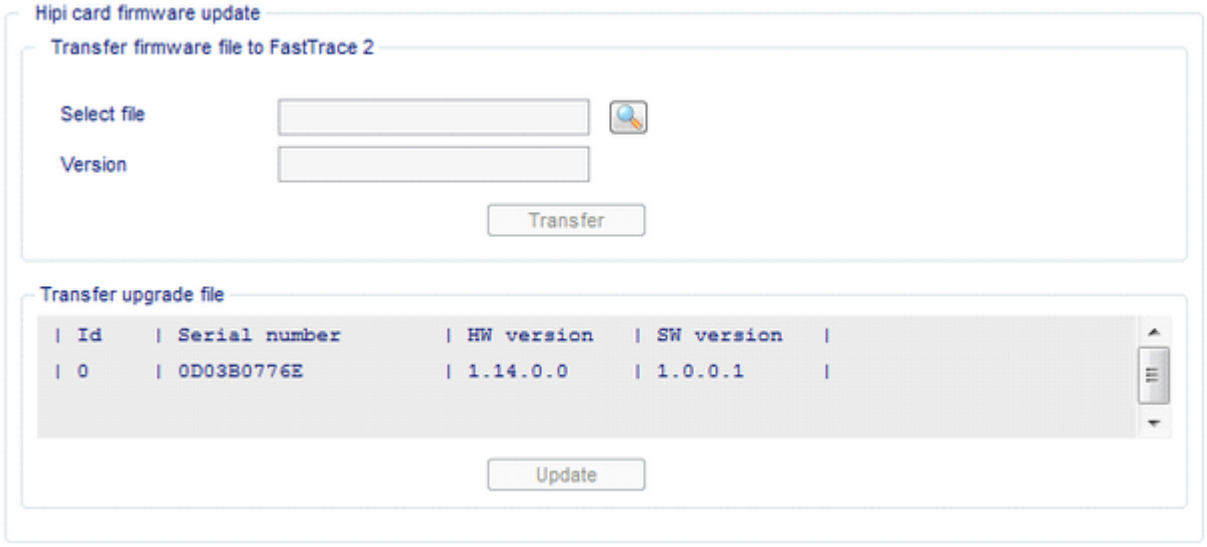
To configure the HIPI card, open **System > Maintenance > HIPI config**. Select the desired HIPI card from the list and click **Configuration**. Enter the correct IP address and corresponding subnet mask. Click **OK** and **Save**.



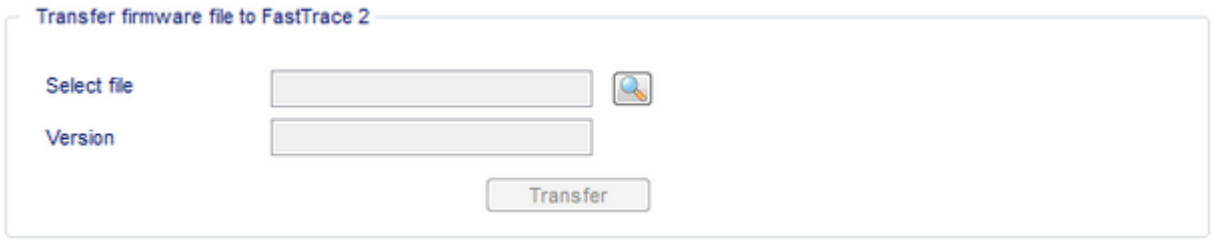
Connect the HIPI card to ETH1 or ETH2 of the FastTrace 2 server, not to ETH0!

Software update

The HIPI card requires software. You can see the software version in the lower window pane of the HIPI configuration window.


Hipi card firmware update
Transfer firmware file to FastTrace 2
Select file
Version
Transfer
Transfer upgrade file
| Id | Serial number | HW version | SW version |
| 0 | 0D03B0776E | 1.14.0.0 | 1.0.0.1 |
Update

To update the HIPI card to a more recent version of the software, open **System > Maintenance > HIPI config**. In the section “Hipi card firmware update” click and open the folder that contains the new version. The update file has the extension ***“.hui”***. Select the file en click ‘Open’.



The version of the software you have uploaded is shown. Click 'Transfer' to upload the new software version to the HIPI card. Once available in the HIPI card, the new software can be updated.

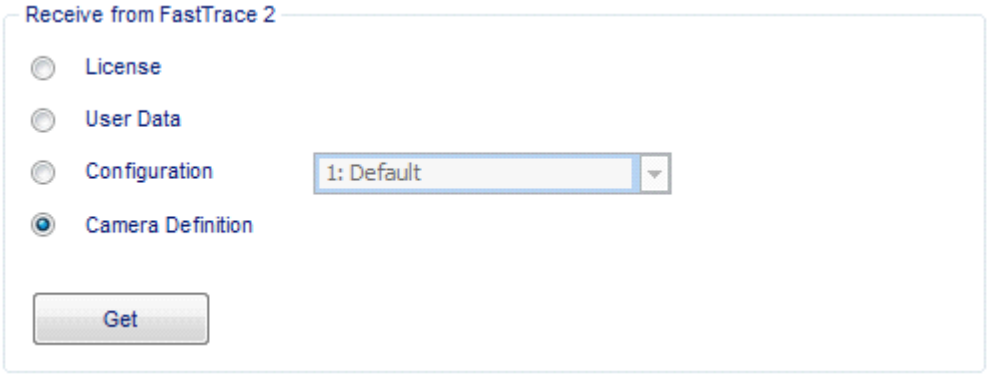
4.4 Supported IP cameras

It is recommended to use the latest firmware version of the camera. Older firmware versions may cause issues with the overall FastTrace 2 performance.

IP cameras are expected to perform best at their latest firmware version, please check the manufacturer's website. In the exceptional case the new cam firmware would not be backwards compatible with its previous version(s) as originally tested with FastTrace this may affect FastTrace2 operation. In these circumstances Xtralis will make the best effort to correct the situation in a reasonable amount of time.

Newer firmware versions than the ones originally tested may show incompatibilities. Please contact the Xtralis Support Division if you encounter any issues. Xtralis will make the best effort possible to address the problem in a reasonable time frame. Although not likely, some camera firmware updates may be incompatible and thus impossible to support on the FastTrace 2.

For an updated list of IP cameras, supported by your currently used version – including the number of video streams they can handle – click **System > Maintenance > Transfer**. In the section "Receive from FastTrace 2" select 'Camera definition' and click 'Get'. A text file with extension ".def" will be created in your work folder.



For an updated list of IP cameras, supported by the most recent FastTrace 2 video system, download the document "Supported IP cameras" at the website http://www.xtralissecurity.com.

Remark:

For the Axis Q7401 video encoder you have these possible options:
- Video in;
- Audio in over IP; Audio out via FastTrace 2;
- All inputs; All outputs;
- PTZ control.

Downloading the compatible camera manufacturer driver is required!

Mind:

When using ACTI IP cameras, you need to turn off the B2 frame option on the camera!

4.5 Video streams

IP cameras can transmit 2 to 4 video streams simultaneously, each with its unique quality, depending on the performance.

Video streams are handled as follows:
- 1 video stream is used for event recording;
- 1 video stream is used for continuous recording;
- 1 video stream is used for analytics (motion detection, tamper detection, quad alarm, postmotion, loitering, video out, …);
- 1 video stream is used for live viewing.

When your model supports only 2 streams, only event recording quality can be selected freely. Continuous recording will use the video stream intended for analytics and live video quality can only be set to one of the two available video streams.

When your model supports only 3 streams, continuous and event recording quality can be defined independently, but the quality of live video can only be set according to one of the three available video streams.

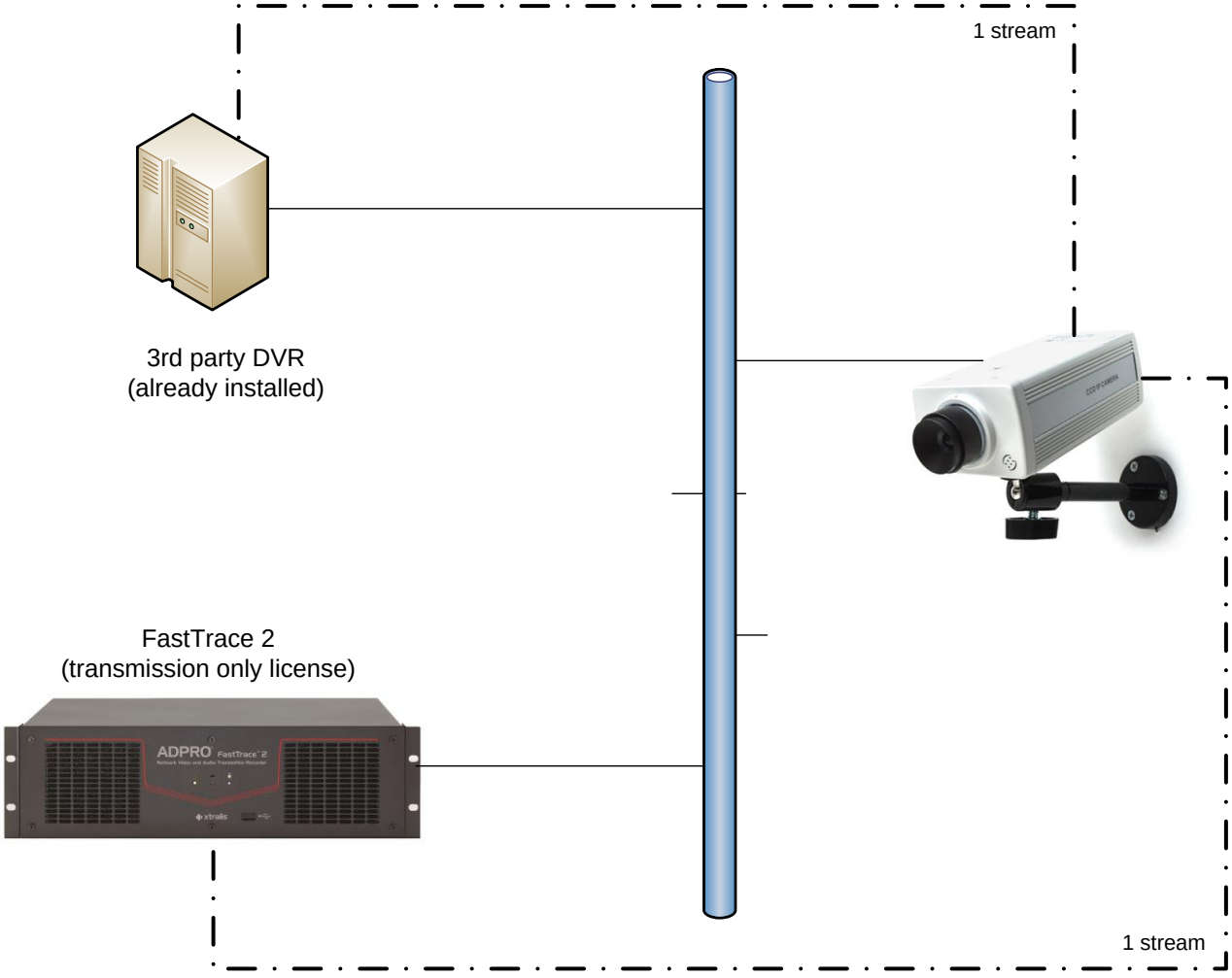
Remark:

Arecont cameras do not support the analytics stream, so motion detection, quad alarm, postmotion, loitering, video out ... etcetera is not supported.

Important:

No other streams may be drawn from the IP camera than those destined for the FastTrace 2! If you do need to draw streams from the IP camera for another application or tool, please tick the option *Treat this cam as a single stream cam* when activating the IP camera.

If you tick the option *Treat this cam as a single stream cam*, only one stream will be used for all features related to the FastTrace 2 server. This means, however, that there will be specific limitations in the FastTrace 2 video system: the only stream that the FastTrace 2 video system will use is the analytics stream. As a result this will be a CIF resolution at 5 fps (or the minimal quality available on the camera).



You can set the stream number as well, yet this must be checked on site, as this depends on the stream number being used by the other application. Please check the correct number in the camera.

5 Using analogue cameras

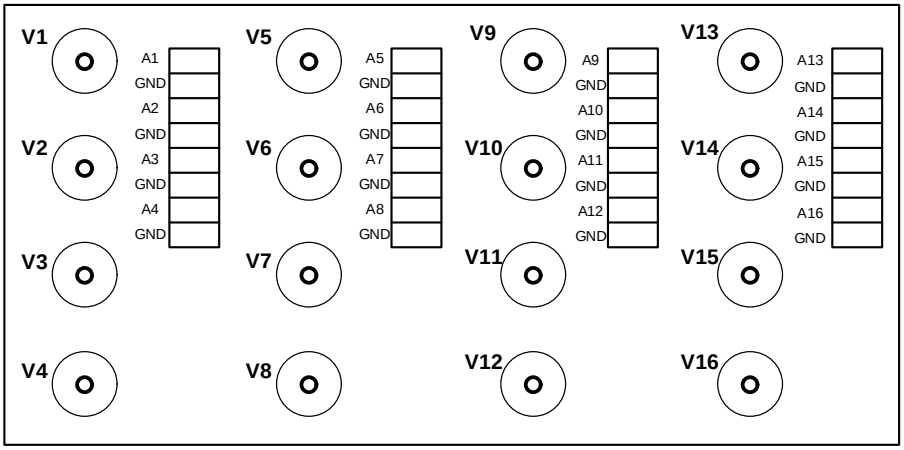
5.1 Technical specifications

Maximum number of cameras	16 (total of analogue and/or IP cameras)
Analogue cameras (*)	4, 8, 12 or 16 analogue A/V inputs Video: PAL or NTSC BNC connectors (1.0 Vp-p; 75 Ohm) Max. cable length: 350 m (RG59); 610 m (RG11) Audio: 1 input per analogue camera Screw connectors Input level: 2.0 Vp-p; 1000 Ohm
Video output	VGA connector; adjustable resolution (up to SXGA)
Video compression	H.264
Audio compression	OggVorbis Codec 16 Kbps (DS40xx cards) OggVorbis Codec G711 (DS42xx cards)
Analogue cameras Video resolution PAL	QCIF (176 x 144) CIF (352 x 288) 2CIF (704 x 288) DCIF (528 x 384) *(not available with DS42xx A/V cards)* 4CIF (704 x 576)
Analogue cameras Video resolution NTSC	QSIF (176 x 120) SIF (352 x 240) 2SIF (704 x 240) DSIF (528 x 320) *(not available with DS42xx A/V cards)* 4SIF (704 x 480)
Analogue cameras images/second PAL	CIF, 2CIF, DCIF: 25 fps / camera 4CIF: 15 fps / camera *(25 fps with DS42xx A/V cards)*
Analogue cameras images/second NTSC	QSIF, SIF, 2SIF, DSIF: 30 fps / camera 4SIF: 15 fps / camera *(25 fps with DS42xx A/V cards)*
Bandwidth	Remotely adjustable: compression, fps and quality. A bandwidth limit can be specified.
Bandwidth consumption	6 fps CIF/SIF: 70 kb/sec 12 fps 4CIF/SIF: 400 kb/sec in optimal quality
Recording type	Continuous, on event (e.g. input, motion detection), alarm over IP (S3100), Presidium
Remote visualisation	Internet Explorer; Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008
PTZ cameras	Several protocols available (*see also* *List of available PTZ protocols*)
Management	- Internet Explorer (installs Client software) - VSKwin software - M3000 software - 3rd party CMS software

(*) *With an ENTRY system license you can only use 4 analogue cameras, because this is the maximum number of analogue cameras that is supported by this specific system license! This is for instance the case with the ADPRO FastTrace 2 Lite.*

5.2 Video & Audio Connections

Analogue cameras can be connected to the rear of the FastTrace 2 video system using a BNC connecting RG59 or RG11 cable.

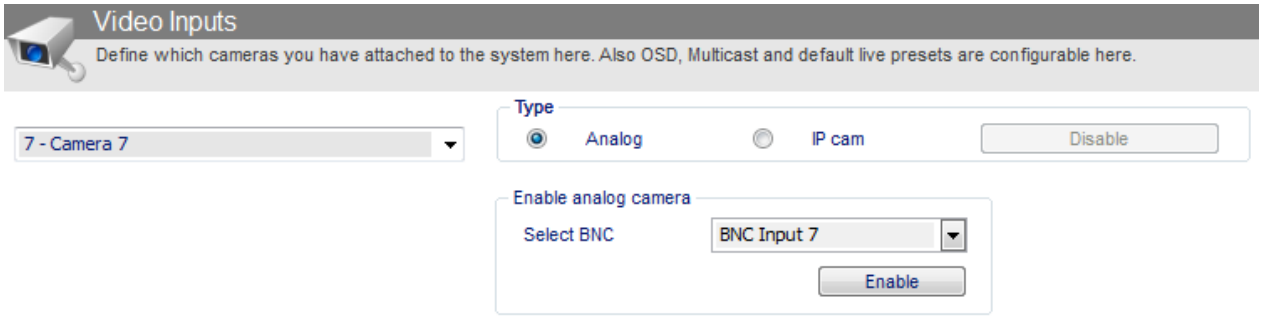


Each camera needs a separate BNC input! Depending on the configuration of your FastTrace 2 server, you will have either 4, 8, 12 or 16 analogue BNC camera inputs.

See The Xtralis configurations for more information on the possible configurations of the FastTrace 2 server.

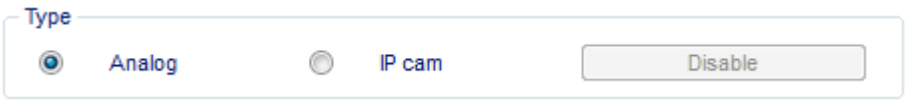
5.3 Camera Configuration

To add an analogue camera, you need to connect the camera to the video system and open **System > Connections > Video inputs**. Then choose a free camera number from the dropdown list:

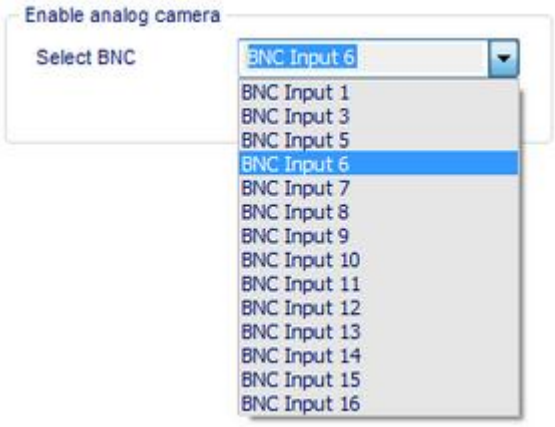


Up to 16 cameras can be connected to the FastTrace 2 video system. For every analogue camera 1 A/V input is required.

Tick the *Analog* option:



Select the BNC input and click **Enable**.



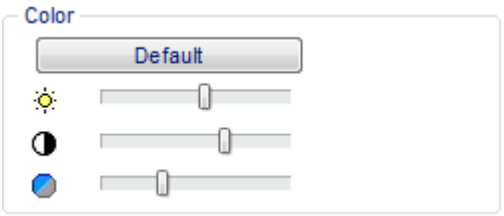
When enabled you can adjust some parameters.

5.3.1 General parameters

Name	Enter a description for the camera (max 20 characters). *It is recommended to use a meaningful and relevant description.*
PIR integrated on camera	Check this option when a PIR has been integrated on this camera.

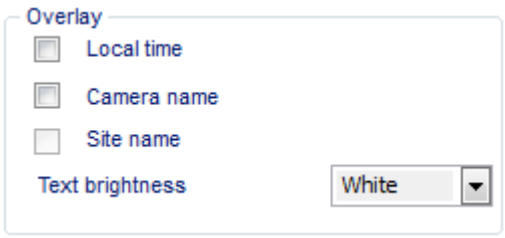
5.3.2 Video settings

5.3.2.1 Color



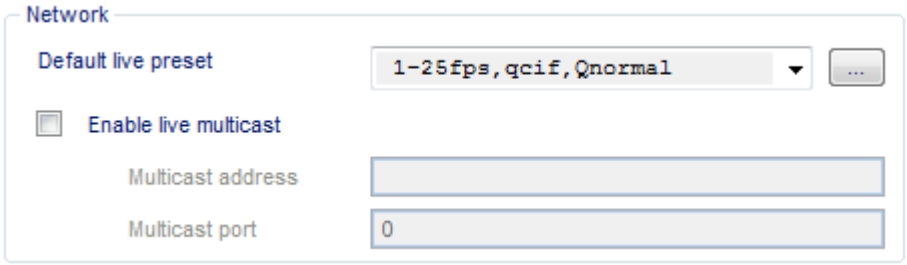
If the image does not provide enough quality, you can adjust brightness, contrast and hue in the “Color” section.

5.3.2.2 Overlay



Local time	Tick this option if you want to visualize the local time on the camera's live image.
Camera name	Tick this option if you want to visualize the camera name on the camera's live image.
Text brightness	This option is not available for IP cameras. The parameter can be added to the IP camera settings via the camera's web browser.
Site name	Tick this option if you want to visualize the site name on the camera's live image.

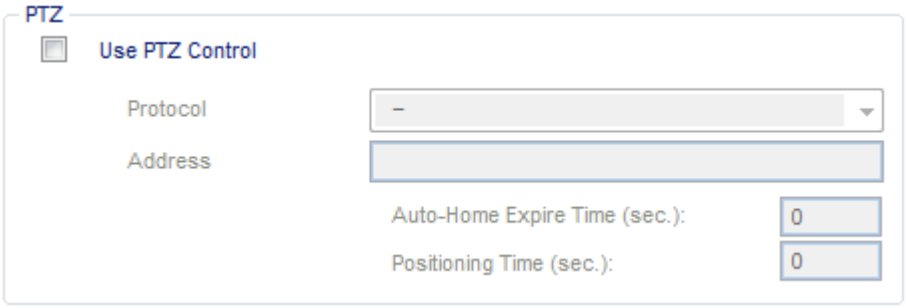
5.3.3 Network



Default live preset	When watching live images from a camera, the image quality can be adjusted at any time by clicking your right mouse button. The initial quality, applied the first time you select the camera, can be specified with this parameter. You can choose from different preset qualities, depending on the camera. If you choose "Hard disk stream", live pictures will follow the same quality as continuous recordings. This way, only two streams are required.
...	With certain types of cameras this button becomes active. Via this button you can open the list with possible quality presets. The parameters you can modify here, are: - Frames per second (fps) - Resolution of the picture - Quality: VBR quality (Qlow, Qnormal of Qhigh) or CBR bit rate (20 through 2048 kbps). The higher the value, the better the quality, but also the higher the bandwidth use! *Remark: for stable image quality VBR is recommended.*
Only live multicast	Multicast is the simultaneous supply of information to one or more computers through only one data stream from the source. When multiple computers poll this one stream, multiple copies will be created, but the initial upload will remain the same. Multicast thus ensures less data traffic over the network. The 224.0.0.0 through 239.255.255.255 address range has been assigned for multicasting on the local LAN network. Tick this option if you want to use the multicast protocol.
Multicast address	Enter the address to which the FastTrace 2 video system has to send the multicast. ***Mind***: every camera should be assigned to a unique multicast address.

	Everyone who has subscribed to the multicast, can view the live images on this address, using a web browser or a FastTrace 2 Client.
Multicast port	Enter the multicast port through which the FastTrace 2 has to send the stream. ***Mind***: every camera should be assigned to a unique multicast port. This port must be defined by the IT Department before connecting the FastTrace 2.

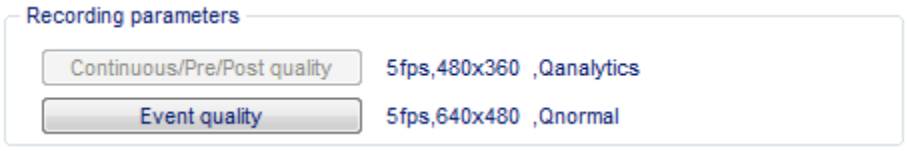
5.3.4 PTZ



Use PTZ Control	Tick this option if you have installed a PTZ camera.
Protocol	Choose the corresponding protocol for the camera you have installed.
Address	Enter the correct camera address for the camera you have installed. Check the camera settings to know the camera address.
Auto-Home Expire Time (sec)	This value indicates the time in seconds that has to be expired after every PTZ action, before the PTZ camera will move back to its home position. If the value is left to 0, the Auto-Home feature will be disabled.
Positioning Time (sec.)	PTZ preset positions can be selected via an input. When that input triggers the PTZ action, the camera will move to the configured PTZ preset position, but the alarm message of the input will be delayed until the PTZ preset positioning time has expired. Thus no blurry images are recorded for quad images.

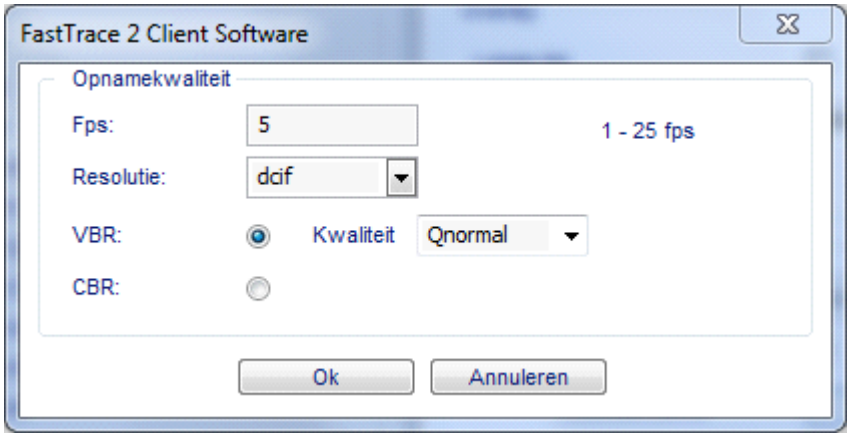
See PTZ settings for detailed information on how to install the Pan Tilt Zoom options…

5.3.5 Recording



Continuous/Pre/Post quality	This shows the quality that has been configured for continuous recordings and for pre and post event recording.
Event quality	This shows the quality that has been configured for the event recording.

Set the recording parameters by clicking the desired quality.



- Fps: the number of images (frames) per second (1 – 25);
- Resolution: the number of pixels per image; depends on the camera type;
- VBR: selects a variable bitrate compression (Qlow, Qnormal or Qhigh);
  CBR: selects a compressed bitrate compression (value 20 – 2048 kbps); the higher the value, the higher the compression and the higher the loss of quality; the compression levels will differ according to the constant data flux in which the file size is predictable, but the quality will depend on the video contents.
  VBR with Qnormal quality is recommended!

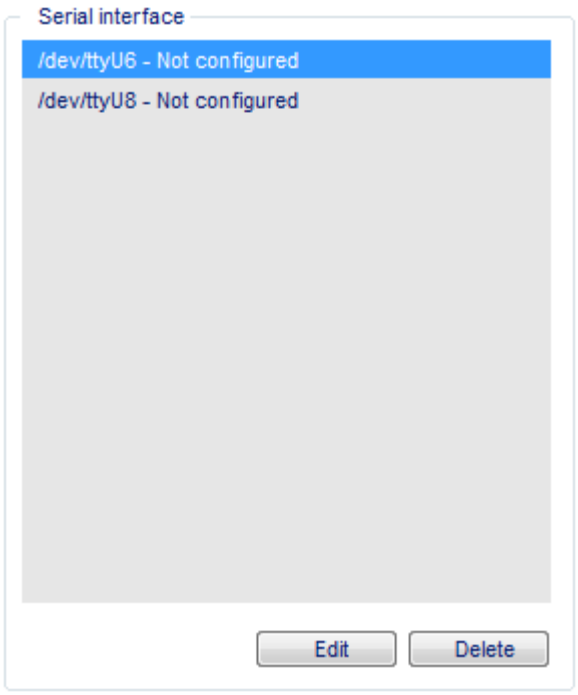
Click **Save**.

5.4 PTZ settings

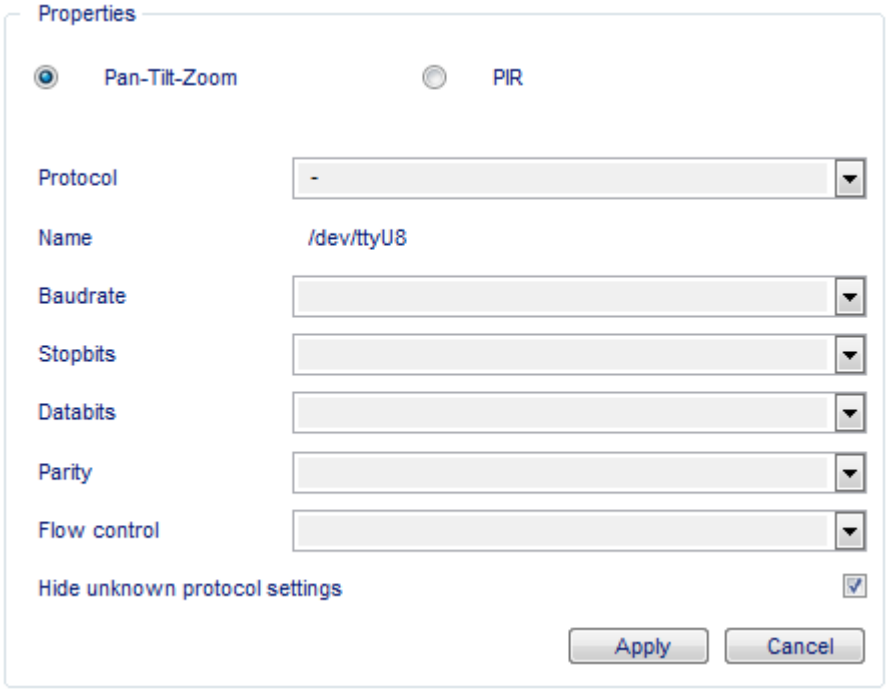
5.4.1 Serial PTZ

Open the *Serial Ports / PTZ* window via **System > Connections > Serial Ports / PTZ**.

Select the serial interface and click **Edit**.



Choose the correct option: *Pan-Tilt-Zoom*.



Select the desired protocol, depending on the camera type. Enter baudrate, stopbits, databits, parity, flow control according to the camera specifications. Normally the settings are correct when choosing the protocol. Untick the option *Hide unknown protocol settings* if you want to modify the default settings.

Click **Apply** and **Save** to maintain any modifications.

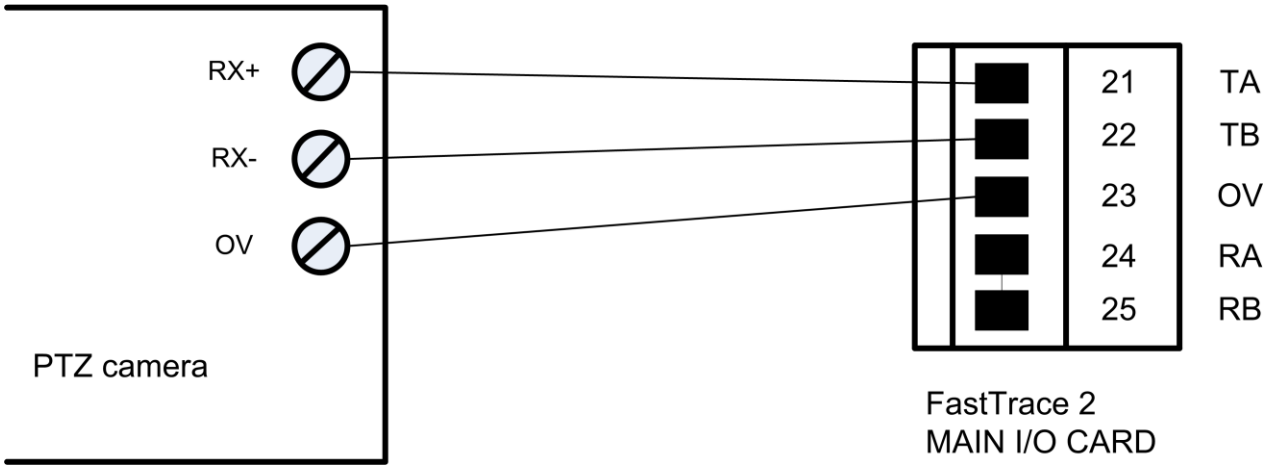
Mind:

The external USB ports, used for PTZ control, can be found at the rear of the FastTrace 2 server. A convertor to convert USB to RS232 or RS485 is required.

When using internal Main I/O cards, the PTZ control can be selected as **/dev/ttyU6** (for the first Main I/O card) and **/dev/ttyU8** (for the second Main I/O card).

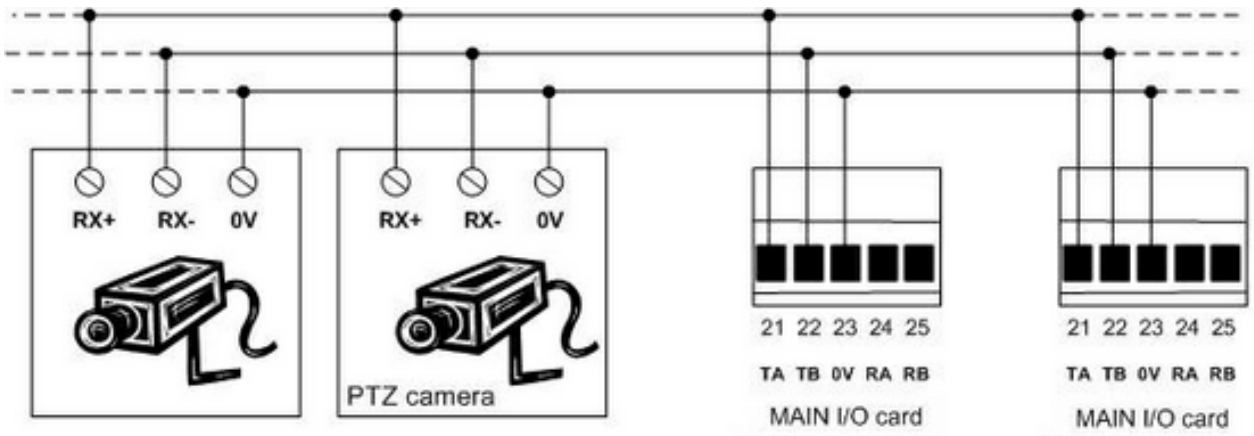
IMPORTANT:
Telemetry station manufacturers provide a variety of models and features. The FastTrace 2 provides PTZ control ability for a number of popular models and where possible, supports the features provided by the manufacturer. Due to the number of models available on the commercial market, details of connection and use for individual models have been provided in this manual. Xtralis does, however, have “tech tips” available for these cameras on the website http://www.xtralissecurity.com.

5.4.2 Serial PTZ on MIO card



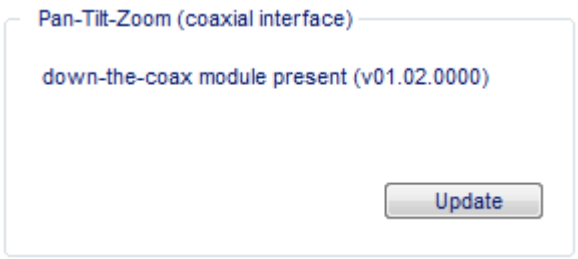
Mind:

If connecting PTZ cameras from the same RS485 to multiple FastTrace 2 servers, change the strap settings on the MIO to RS485 – 2 wires (PTZ). Maximum cable length of the RS485 cables is 1200 m.



5.4.3 DTC PTZ

Open the PTZ window via **System > Connections > Serial Ports / PTZ**. Check if the DTC card is present.



Remark:

The current software version loaded in the DTC card is shown in the list. To update the DTC card to a more recent software version, open **System > Connections > Serial Ports / PTZ**. Click 'Update' and locate the file "dtc.img" with the latest software. Click **Apply**.

These PTZ protocols are supported on the DTC card:

- Down-the-Coax (Pelco Ext.)
- Down-the-Coax (Baxall Std.)
- Down-the-Coax (Baxall Alt.)
- Down-the-Coax (BBV coax)

5.4.4 List of available PTZ protocols

These PTZ protocols are supported by the FastTrace 2 video system:

- 360 Vision / Vantage Juno / VT Fastrax-P / Xeno Neodome
- Amux IEC
- Baxall ZMX
- Baxall ZTX
- BBV
- Burle / Philips / Bosch
- COHU
- Conway
- CS Lilin
- CS Lilin2
- Dennard 2050
- Diamond
- Digital Sprite
- Elbex
- Ernitec
- GPS
- Grundig
- Harris
- JVC
- Kalatel
- Mark Mercer
- Molynx
- Molynx Variable Speed
- Pacom
- Panasonic (conventional)
- Panasonic (new)
- Pelco D
- Pelco P
- Samsung
- Sensormatic
- Sensormatic Controller
- Sensormatic Speeddome VII
- Siemens
- Synectics
- Unidex
- VCL
- Vicon
- Video Switch
- Visca
- Vista Powerdome

Attention:

- When using the Pelco Spectra Cam 4 the PTZ address has an offset of -1 in the FastTrace 2.
- When using the JVC protocol the PTZ address has an offset of +1 in the FastTrace 2.

Example:

When using a JVC protocol with address 1 in the FastTrace 2, the PTZ address of the camera should be 2.

5.5 USB convertors

Device	Order number	Pin assignment
USB to RS485 convertor	20415490	RS485 Pin assignment (DB9 male connector) 1 485- 2 485+ 5 GND
USB to RS232 convertor *RS232 is only used on some PTZ cameras (such as the Philips G3 Autodome camera). Cable length is limited to 50 feet. If more than 50 feet the cable capacitance should be kept below 2500 pF.* *pF = pico farads*	20415510	RS232 Pin assignment (DB9 male connector) 1 Received Line Signal Detect 2 Received Data 3 Transmitted Data 4 DTE Ready 5 Signal Ground 6 DCE Ready 7 Request to Send 8 Clear to Send 9 DCE Ready

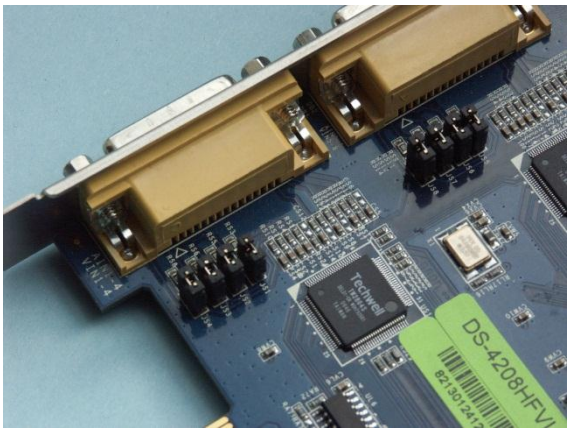
Important:

You need to reboot the FastTrace 2 server after connecting the convertor!

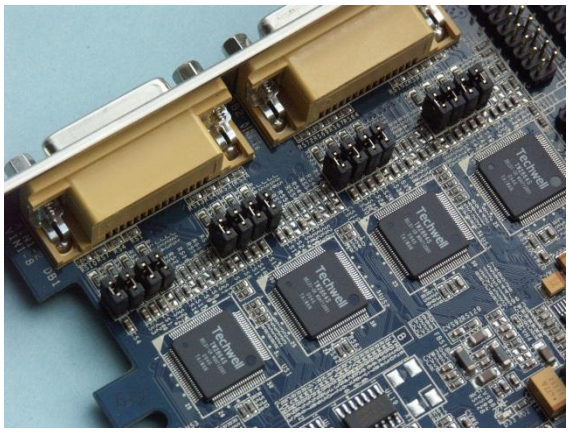
5.6 Video input termination (75 Ohm / High impedance)

This is only available on the latest version of the 8 or 16 channel video cards!

Jumpers JP1 – JP8/16 determine whether the corresponding video input is terminated with 75 Ohm (when strap is placed) or not (when strap is removed).



8 channel AV card

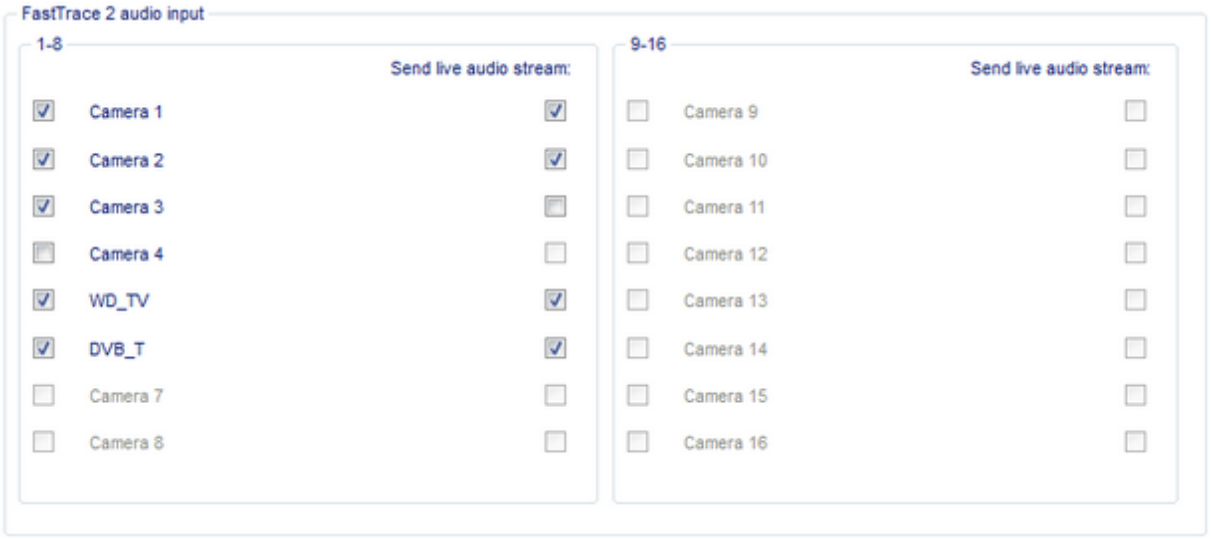


16 channel AV card

6 Audio

6.1 Audio IN

Open the “Audio” window via **System > Connections > Audio**. Tick all inputs that have audio connection.



The option “Send live audio stream”, to enable live audio streaming on the camera, should be disabled if bandwidth connections are low.

6.1.1 Recommended microphones

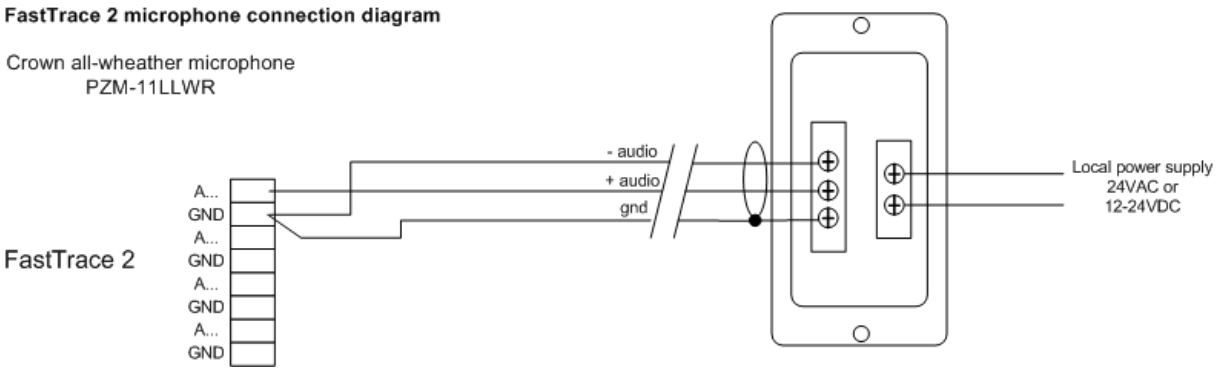
These microphones have been tested and approved:

6.1.1.1 Crown all-weather PZM-11LLWR

6.1.1.1.1 Specifications

- Technology: electret condenser
- Designed for outdoor use: -10 ~ +60°C
- Power supply: 12 ~ 24 VAC or DC
- Current consumption: 4mA
- Dimensions: 11.5 x 7 x 4.4 mm

6.1.1.1.2 Wiring diagram

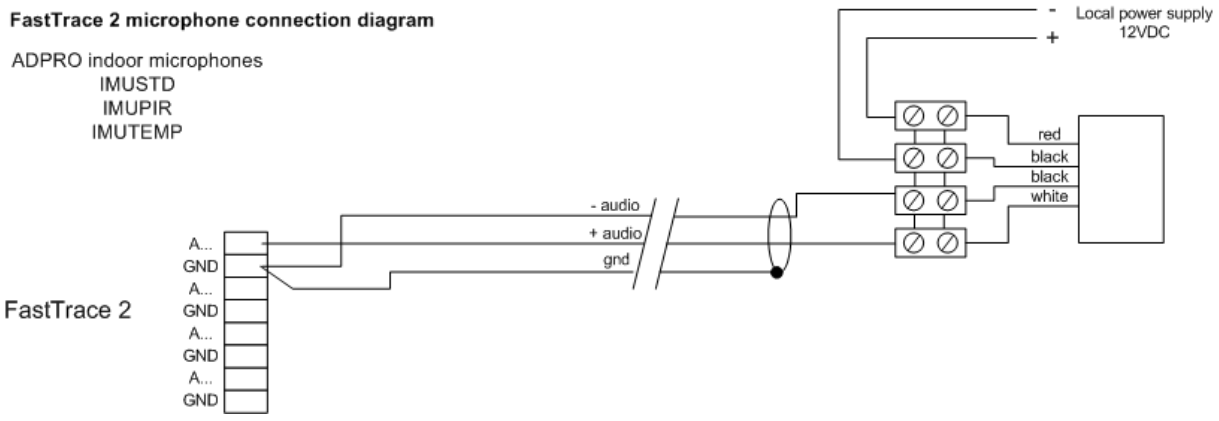


6.1.1.2 ADPRO microphones IMUSTD; IMUPIR; IMUTEMP

6.1.1.2.1 Specifications

- IMUSTD = standard microphone
  IMUPIR = microphone with PIR detector appearance
  IMUTEMP = microphone with heat detector appearance
- Designed for indoor use
- Power supply: 12 VDC from regulated power supply
- Current consumption: 200 ~ 400 mA

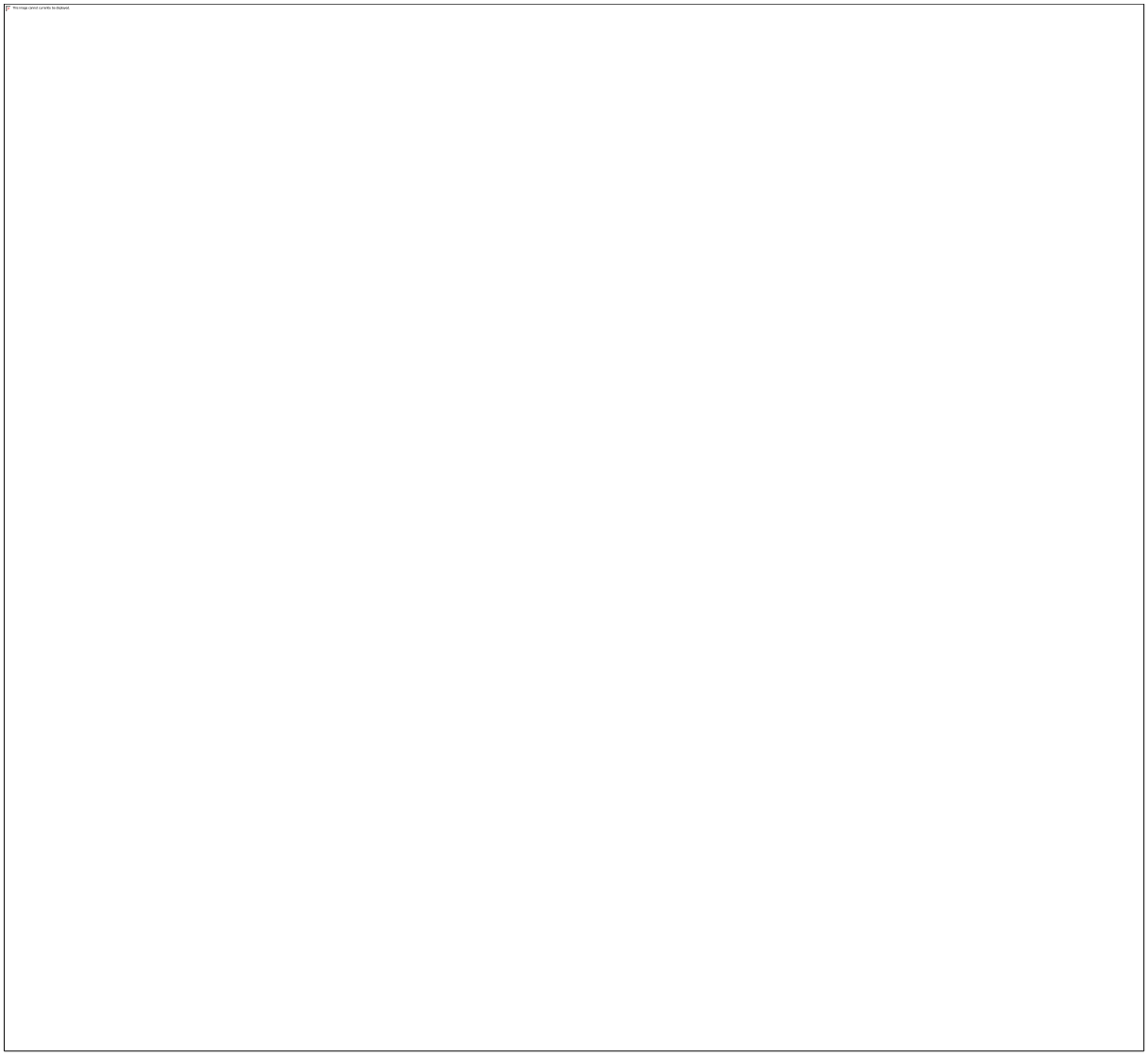
6.1.1.2.2 Wiring diagram



6.1.1.3 ADPRO Audio Unit

See “Technical data sheet 19531950 – ADPRO Audio Unit”.

6.1.1.3.1 Wiring diagram



6.2 Audio OUT

Audio outputs are available on one or two VM22A units, connected in cascade. Unit 0 is controlled by the MIO card that is inserted in the video system and drives the loudspeakers 1 to 10. Unit 1 connects to the first unit through the EIO loop connecter and drives loudspeakers 11 to 20.
(See the *VM22A Audio Switcher - Installation and User Manual* for more information)

Each loudspeaker is associated to the camera with the matching number. Loudspeakers 17 to 20 are not selectable since the video system is limited to 16 cameras.

To talk back to a person on the remote site, launch the FastTrace 2 Client, open the LIVE page and select the desired camera by clicking on its image. By default the "Push to talk" mode will be active: click and keep it pressed down (with the left mouse button). You can now start talking through the microphone that is connected to the MIC input of the computer. When the option "Full duplex mode" has been ticked, the "Push to talk" mode will be disabled. In this case you can activate the audio by simply clicking the icon. To deactivate the audio mode you need to click the icon again.

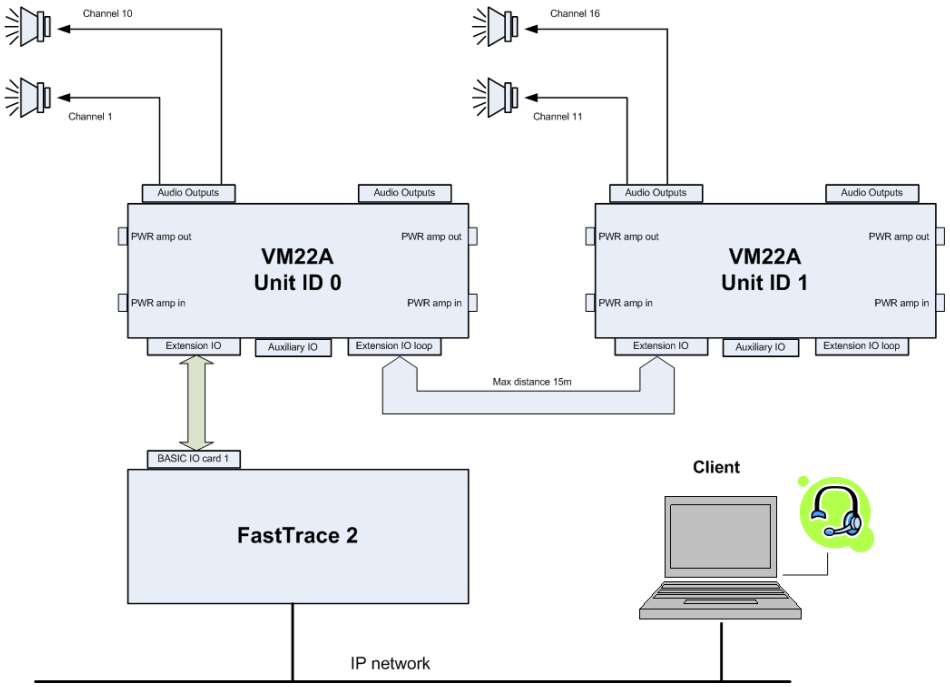
Make sure the audio output parameters are correct. Open **System > Connections > Audio** to modify the settings. Mind that the audio IN option must be activated if you want to use Audio OUT.

Enter the audio server port (by default port 3000) that will be used to transmit audio from the Client to the FastTrace 2 Server. Also select the desired protocol (by default UDP) that will be used to transmit the audio.

If you want to force duplex mode to allow communication in both directions, tick the option *Full duplex mode*. The *Push to Talk* mode will be disabled when this option is ticked!

Click **Save**.

If only 1 loudspeaker is needed on the site, you can do without the VM22A switch. In this case, connect an amplified loudspeaker to the audio out plug of the motherboard (= green 2.5'' jack jack). It is also possible to connect an amplified loudspeaker to the audio out output on the Main I/O Card.



Remark:

If talk-back does not work, check the following:

1) Routers may block UDP packets. Use TCP or configure the router to allow UDP packets.

2) Use the PC headphones plug instead of the PC microphone plug.

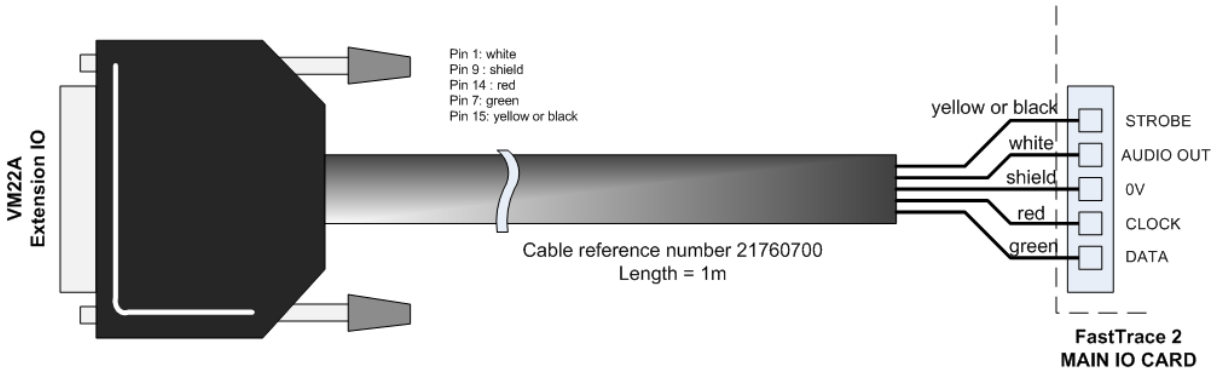
3) The microphone on your computer is not correctly configured. In this case you need to configure the microphone device:
In Windows XP:
- In **Control Panel**, select **Sound and Audio Devices**;
- Open the **Voice** tab in the **Sounds and Audio Devices Properties** dialog box;
- Check whether the **default device** is the device you want to use for the FastTrace 2;
- Next, click the **Volume** button under the **Voice recording** heading;
- Adjust the vertical volume slide on the **Mic volume** or **Line volume**, depending on which device you are using;
- Click 'OK' and close the **Control Panel**;
- Test with **Sound Recorder**.

In Windows Vista / Windows 7:
- Open **Control Panel** and click **Hardware and Sound**;
- Open the **Recording** tab in the **Sound** window;
- Right click on the microphone device you plugged in and select the '*Set as default device'* option;
- To test and see if it really works, tap the microphone with your finger a few times. In the **Sounds** window, the empty lines next to the default microphone should fill up with a green colour.

6.2.1 Connecting the VM22A audio switch to the FastTrace 2 video system

A specific cable is used to connect the VM22A to the FastTrace 2 video system.

On the back of the FastTrace 2, locate the MIO card. Connect the cable to the MIO as illustrated underneath. Please respect the colours code (yellow = STROBE; white = AUDIO OUT, shield = OV, red = CLOCK and green = DATA).



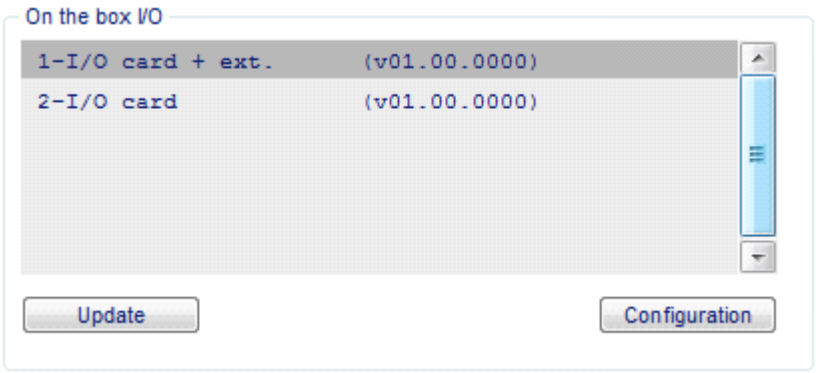
7 I/O Cards Configuration

7.1 Internal I/O Cards

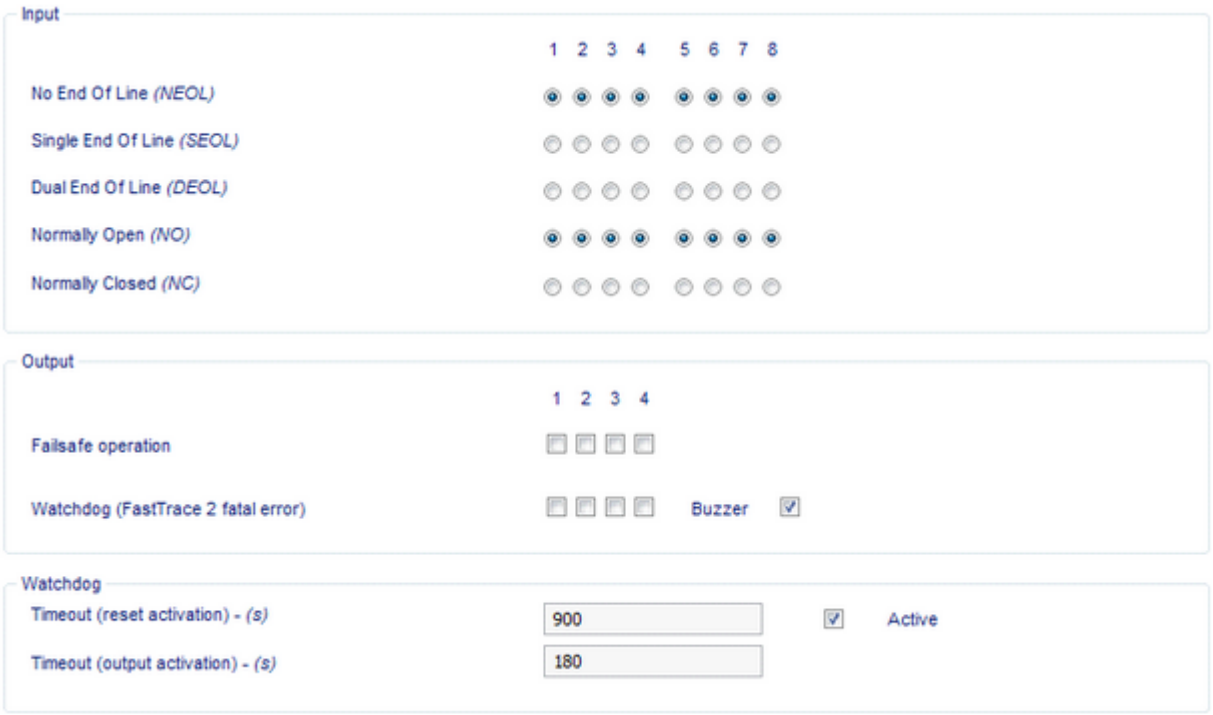
OTB I/O (On The Board Inputs & Outputs):

- Internal Main I/O card (MIO) and Extension I/O card (EIO), offering 20 balanced inputs, 8 relay outputs and control signals for either VM22A equipment (audio output switcher) or PTZ cameras (RS485 output).
- Second set with MIO and EIO card possible to double the number of inputs to 40 and the number of outputs to 16. This also adds an output for PTZ cameras.

All connected OTB (On The Board) IO cards are automatically detected by the FastTrace 2 server. To configure these inputs and outputs, open the Internal I/O window via **System > Connections > I/O**.



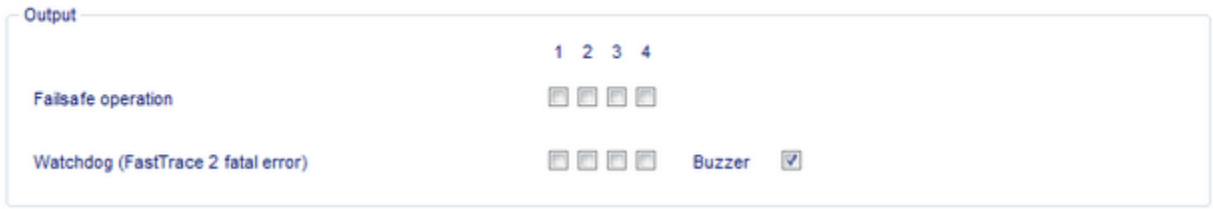
Select an I/O card from the list and click ‘Configuration’.



Configure the inputs as NEOL/SEOL/DEOL with NO or NC contact.
(*see technical datasheet 19531920 – Main and Extension I/O cards*)

Input
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
No End Of Line (NEOL)
Single End Of Line (SEOL)
Dual End Of Line (DEOL)
Normally Open (NO)
Normally Closed (NC)

Configure the outputs as Normal or Failsafe operation. If Failsafe operation, the relay is activated during idle state and drops when the output is driven. The advantage is that Failsafe outputs will drop to 'alarm state' when the power supply is cut.



You can also configure outputs for Watchdog operation. These outputs will be activated when the I/O card can't be reached by the video system for some time, as specified with the parameter Timeout (output activation). This situation can occur if the video system hangs. Timeout values are specified in seconds.

Optionally the buzzer can be activated during a watchdog alarm.

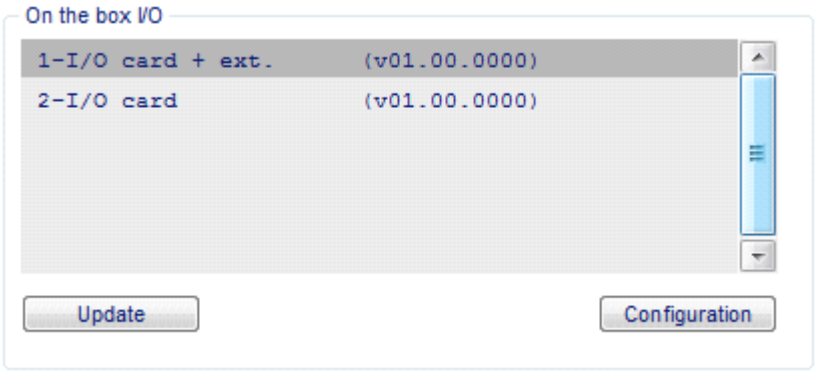
Click 'OK' to save the new settings or 'Cancel' to return to the previous window.

Mind:

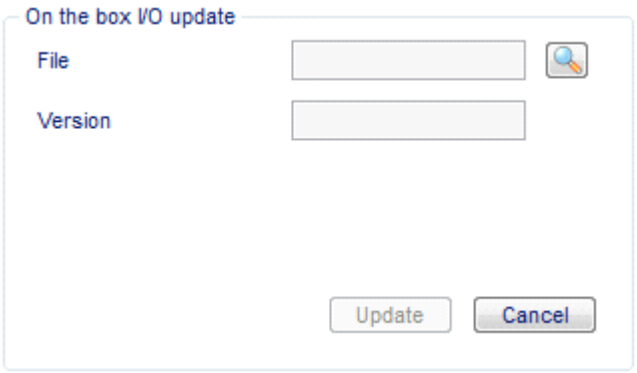
With an ENTRY system license only 1 Main I/O Card can be installed. Multiple Main I/O Cards are not supported. Also Extended I/O Cards are not supported when using the ENTRY system license! This is for instance the case with the ADPRO FastTrace 2 Lite.

7.1.1 Update Main I/O card

The current software version, loaded in the MIO card, is shown in the list.



To update the MIO card to a more recent software version, open **System > Connections > I/O**, select the desired MIO card and click ‘Update’. On the right a new section appears:



Locate the file “usbio.img” (with the latest software version) via . The version of the selected file is shown. Click ‘Update’ to load the new version in the MIO card.

7.1.2 USB I/O address range

Main I/O and Extension I/O: set 1

I2560	IO card absent	C2560	green LED *
		C2561	yellow LED *
		C2562	blue LED *
		C2563	buzzer *
I2576 / I2596	alarm / tamper on input 1	C2576	output 1
I2577 / I2597	alarm / tamper on input 2	C2577	output 2
I2578 / I2598	alarm / tamper on input 3	C2578	output 3
I2579 / I2599	alarm / tamper on input 4	C2579	output 4
I2580 / I2600	alarm / tamper on input 5	C2580	output 5
I2581 / I2601	alarm / tamper on input 6	C2581	output 6
I2582 / I2602	alarm / tamper on input 7	C2582	output 7
I2583 / I2603	alarm / tamper on input 8	C2583	output 8
I2584 / I2604	alarm / tamper on input 9		
I2585 / I2605	alarm / tamper on input 10		
I2586 / I2606	alarm / tamper on input 11		
I2587 / I2607	alarm / tamper on input 12		
I2588 / I2608	alarm / tamper on input 13		
I2589 / I2609	alarm / tamper on input 14		
I2590 / I2610	alarm / tamper on input 15		
I2591 / I2611	alarm / tamper on input 16		
I2592 / I2612	alarm / tamper on input 17		
I2593 / I2613	alarm / tamper on input 18		
I2594 / I2614	alarm / tamper on input 19		
I2595 / I2615	alarm / tamper on input 20		

** Status of front LED indicators and buzzer.*

Main I/O and Extension I/O: set 2

I2560	IO card absent	C2624	green LED *
		C2625	yellow LED *
		C2626	blue LED *
		C2627	buzzer *
I2640 / I2660	alarm / tamper on input 1	C2640	output 1
I2641 / I2661	alarm / tamper on input 2	C2641	output 2
I2642 / I2662	alarm / tamper on input 3	C2642	output 3
I2643 / I2663	alarm / tamper on input 4	C2643	output 4
I2644 / I2664	alarm / tamper on input 5	C2644	output 5
I2645 / I2665	alarm / tamper on input 6	C2645	output 6
I2646 / I2666	alarm / tamper on input 7	C2646	output 7
I2647 / I2667	alarm / tamper on input 8	C2647	output 8
I2648 / I2668	alarm / tamper on input 9		
I2649 / I2669	alarm / tamper on input 10		
I2650 / I2670	alarm / tamper on input 11		
I2651 / I2671	alarm / tamper on input 12		
I2652 / I2672	alarm / tamper on input 13		
I2653 / I2673	alarm / tamper on input 14		
I2654 / I2674	alarm / tamper on input 15		
I2655 / I2675	alarm / tamper on input 16		
I2656 / I2676	alarm / tamper on input 17		
I2657 / I2677	alarm / tamper on input 18		
I2658 / I2678	alarm / tamper on input 19		
I2659 / I2679	alarm / tamper on input 20		

** front LED indicators and buzzer are always controlled by set 1.*

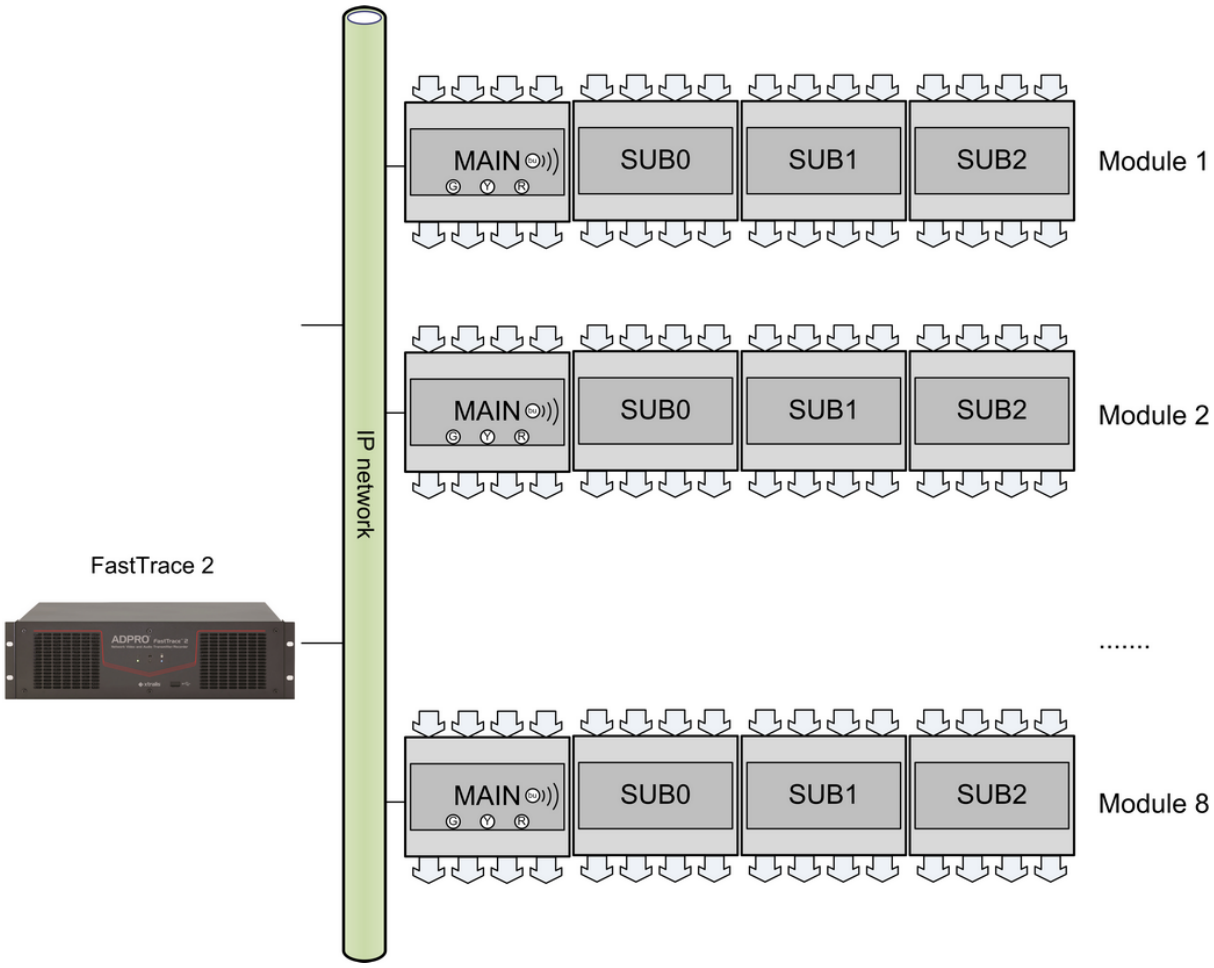
7.2 Net I/O modules

For more detailed information please consult technical data sheet 19531880.

The FastTrace 2 can be linked to 8 Network IO modules. These modules – mounted on a Din Rail installation – are connected to the local network, and powered by PoE or with a local adapter. Each IO module receives a number from 1 to 8 when it is added to the list, and offers 4 inputs and 4 outputs. Each IO module can be extended with 1 to 3 submodules, to obtain up to 16 inputs and outputs.

Network IO modules also have LED indicators and a buzzer which are controlled by the FastTrace 2. Network IO modules return fault conditions on 4 separate addresses. Faults include:

- module is starting up
- module has been reset
- module power fault
- module not present



7.2.1 Net I/O address range

INPUTS

	address								
alarm	1	2	3	4	5	6	7	8	
1	I2050	I2114	I2178	I2242	I2306	I2370	I2434	I2498	**MODULE POWER LOSS**
2	I2051	I2115	I2179	I2243	I2307	I2371	I2435	I2499	**MODULE PRESENCE FAULT**

	Digital INPUT															
address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	I2080	I2081	I2082	I2083	I2084	I2085	I2086	I2087	I2088	I2089	I2090	I2091	I2092	I2093	I2094	I2095
2	I2144	I2145	I2146	I2147	I2148	I2149	I2150	I2151	I2152	I2153	I2154	I2155	I2156	I2157	I2158	I2159
3	I2208	I2209	I2210	I2211	I2212	I2213	I2214	I2215	I2216	I2217	I2218	I2219	I2220	I2221	I2222	I2223
4	I2272	I2273	I2274	I2275	I2276	I2277	I2278	I2279	I2280	I2281	I2282	I2283	I2284	I2285	I2286	I2287
5	I2336	I2337	I2338	I2339	I2340	I2341	I2342	I2343	I2344	I2345	I2346	I2347	I2348	I2349	I2350	I2351
6	I2400	I2401	I2402	I2403	I2404	I2405	I2406	I2407	I2408	I2409	I2410	I2411	I2412	I2413	I2414	I2415
7	I2464	I2465	I2466	I2467	I2468	I2469	I2470	I2471	I2472	I2473	I2474	I2475	I2476	I2477	I2478	I2479
8	I2528	I2529	I2530	I2531	I2532	I2533	I2534	I2535	I2536	I2537	I2538	I2539	I2540	I2541	I2542	I2543
	main module				**sub0 module**				**sub1 module**				**sub2 module**			

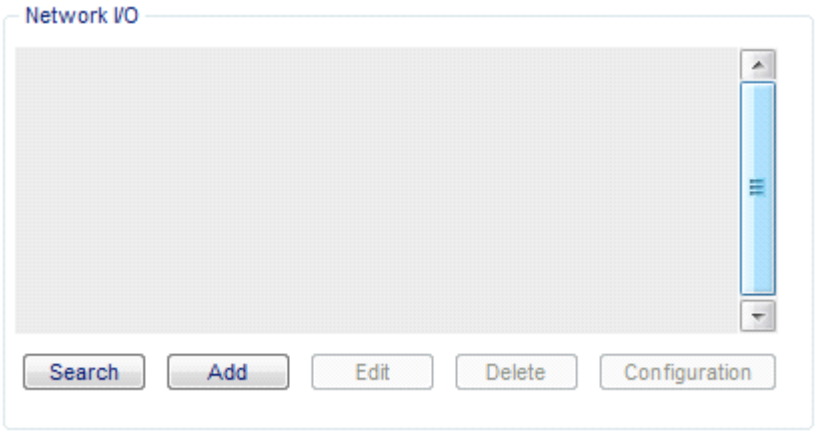
OUTPUTS

	address								
OUT	1	2	3	4	5	6	7	8	
0	C2048	C2112	C2176	C2240	C2304	C2368	C2432	C2496	**GREEN LED**
1	C2049	C2113	C2177	C2241	C2305	C2369	C2433	C2497	**YELLOW LED**
2	C2050	C2114	C2178	C2242	C2306	C2370	C2434	C2498	**RED LED**
3	C2051	C2115	C2179	C2243	C2307	C2371	C2435	C2499	**BUZZER**

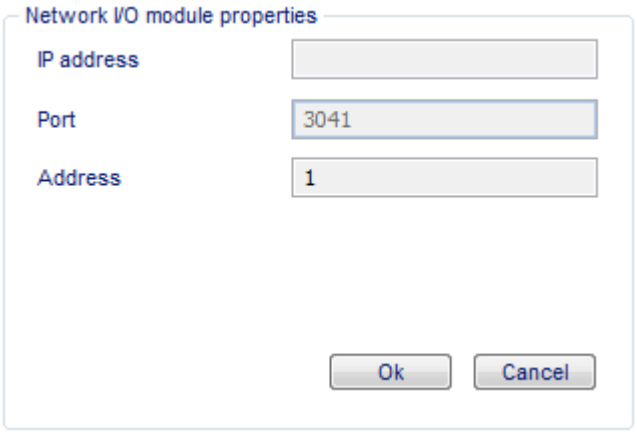
	relays OUTPUT															
address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	C2080	C2081	C2082	C2083	C2084	C2085	C2086	C2087	C2088	C2089	C2090	C2091	C2092	C2093	C2094	C2095
2	C2144	C2145	C2146	C2147	C2148	C2149	C2150	C2151	C2152	C2153	C2154	C2155	C2156	C2157	C2158	C2159
3	C2208	C2209	C2210	C2211	C2212	C2213	C2214	C2215	C2216	C2217	C2218	C2219	C2220	C2221	C2222	C2223
4	C2272	C2273	C2274	C2275	C2276	C2277	C2278	C2279	C2280	C2281	C2282	C2283	C2284	C2285	C2286	C2287
5	C2336	C2337	C2338	C2339	C2340	C2341	C2342	C2343	C2344	C2345	C2346	C2347	C2348	C2349	C2350	C2351
6	C2400	C2401	C2402	C2403	C2404	C2405	C2406	C2407	C2408	C2409	C2410	C2411	C2412	C2413	C2414	C2415
7	C2464	C2465	C2466	C2467	C2468	C2469	C2470	C2471	C2472	C2473	C2474	C2475	C2476	C2477	C2478	C2479
8	C2528	C2529	C2530	C2531	C2532	C2533	C2534	C2535	C2536	C2537	C2538	C2539	C2540	C2541	C2542	C2543
	main module				**sub0 module**				**sub1 module**				**sub2 module**			

7.2.2 Adding Net I/O module with known IP address

Open the *I/O Configuration* window via **System > Connections > I/O**.



Click **Add**. On the right you will see the section *Network I/O module properties* appear.



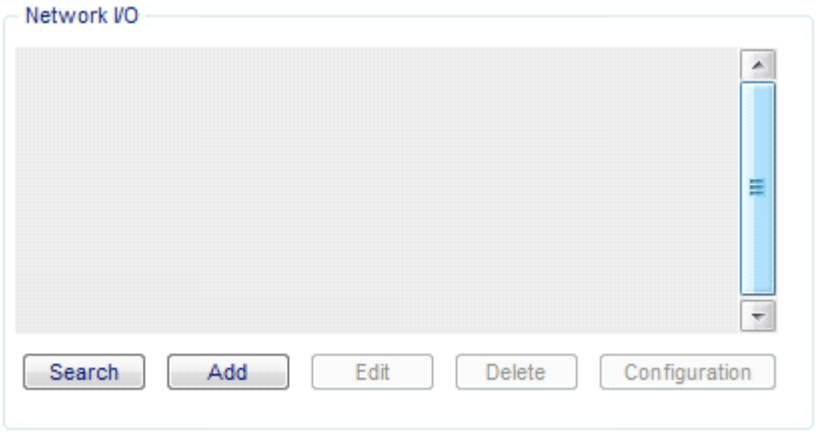
Enter IP address and address (= order number) of the Net IO module (1 – 8). The port number (i.e. the port to which the IO module is listening) cannot be modified.

Click **OK** to add the IO module.

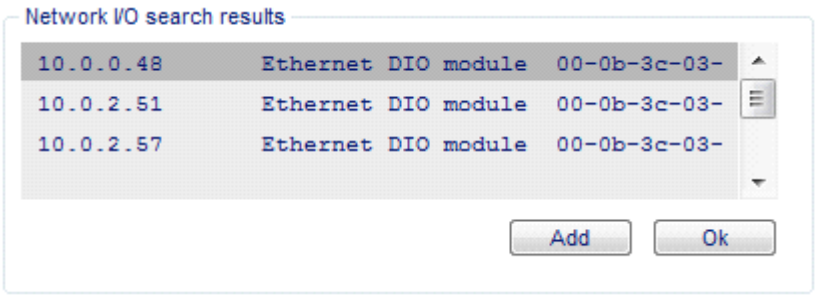
Click **Save** to make sure the modifications are saved.

7.2.3 Searching Net I/O modules on the local network

Open the *I/O Configuration* window via **System > Connections > I/O**.



Click **Search**. Underneath the section *Network I/O search results* will appear.



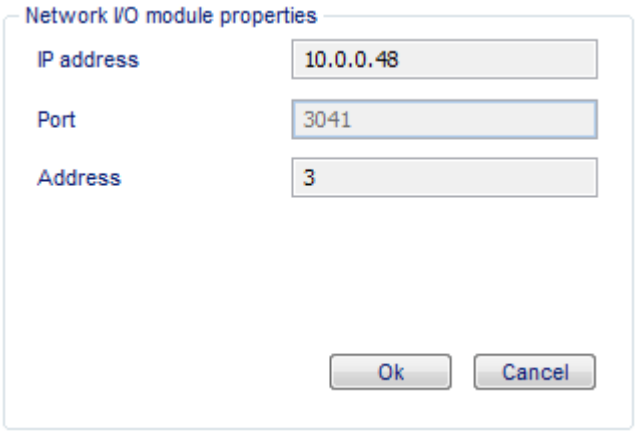
Select the desired IO module and click **Add**. The selected Net IO module is now shown in the list *Network I/O*.

Add all desired Net I/O modules and then click **OK**.

In the list with Network IO modules, select the desired module to edit and/or configure.

7.2.4 Modifying the IP settings of a Net I/O module

Open the *Net I/O configuration* window via **System > Connections > I/O**. Select the desired Net I/O module from the list and click **Edit**.



Enter IP address and Net I/O address (order number 1 -8).

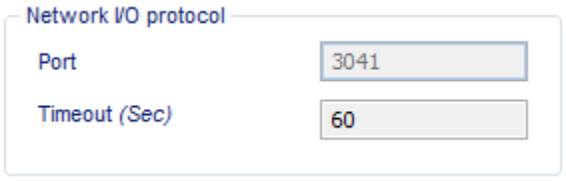
Click **Ok** and **Save**.

7.2.5 Net I/O module inputs & outputs setup

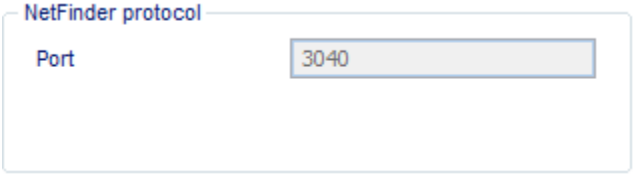
Open the *Net I/O configuration* window via **System > Connections > I/O**. Select the desired Net I/O module from the list and click **Configuration**.

Modify the name of the network IO module. It is recommended to use a meaningful and relevant description.

Modify the port of the Net IO module. This port should be the same port as selected when the IO module was added.



You cannot modify the port used by the Netfinder tool. Netfinder is an external tool used to program the IP address of an IO module and to update its software. You can find this tool on the CD/DVD delivered with the system, or you can download it from the website http://www.xtralissecurity.com.



Digital inputs may be inverted. Normally the input is configured as NO (normally open). If you tick the *Inverted* option, the input will be configured as NC (normally closed).

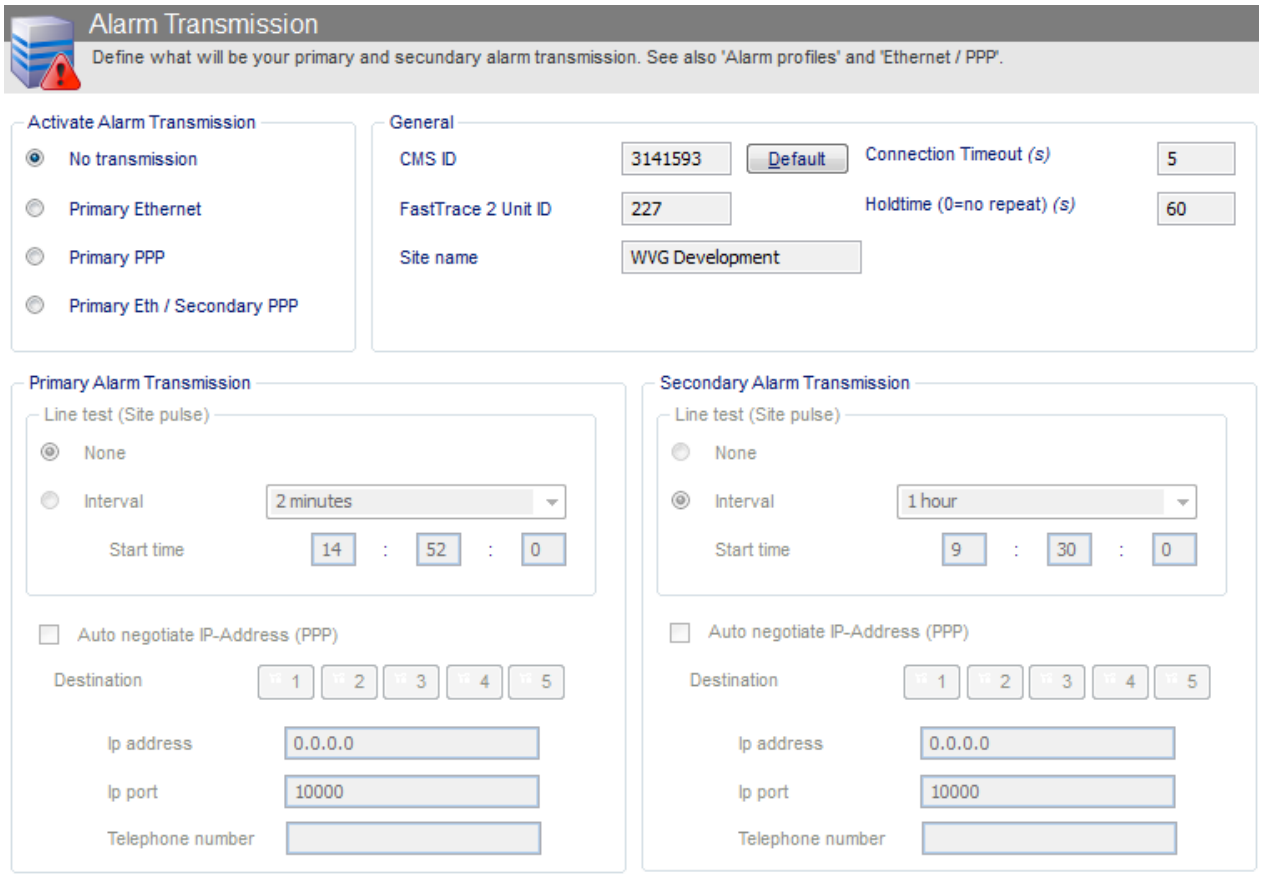
Digital outputs can be configured for failsafe operation and/or watchdog operation. Fail safe operation means that the relay is inverted: the output will be activated when idle. Watchdog operation means that the output will be activated on communication time-out (network IO protocol time out, to be defined via **System > Behaviour > Alarm transmission > General**).

Click **Save**.

8 Alarms

8.1 Alarm transmission

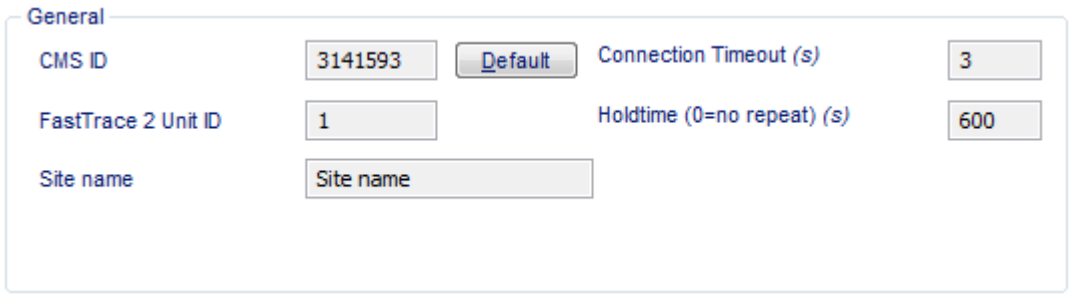
To activate alarm transmission through main channel and/or backup channel, open **System > Behaviour > Alarm Transmission**. Modify the settings and click **Save**.



8.1.1 Default settings

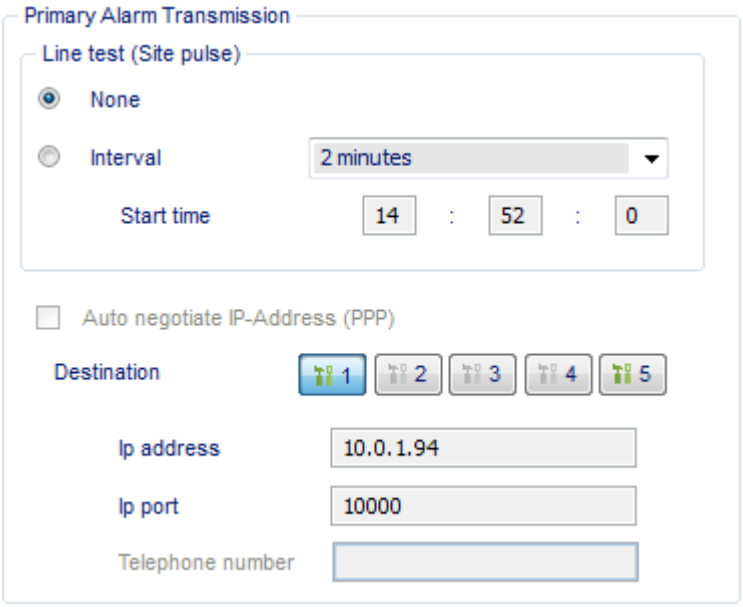
Choose what kind of alarm transmission has to be configured:

Parameter	Description	Default value
Activate Alarm Transmission	○ No transmission; ○ Primary Ethernet: the video server connects to the CMS through a LAN connection; ○ Primary PPP: the video server connects to the CMS through a dial-up connection (requires an external modem connected to USB port /dev/ttyU1); ○ Primary Eth / Secondary PPP: the video server connects to the CMS through a LAN as main connection and a dial-up network as backup connection. The backup connection is used when transmission on the main connection is unsuccessful.	No transmission



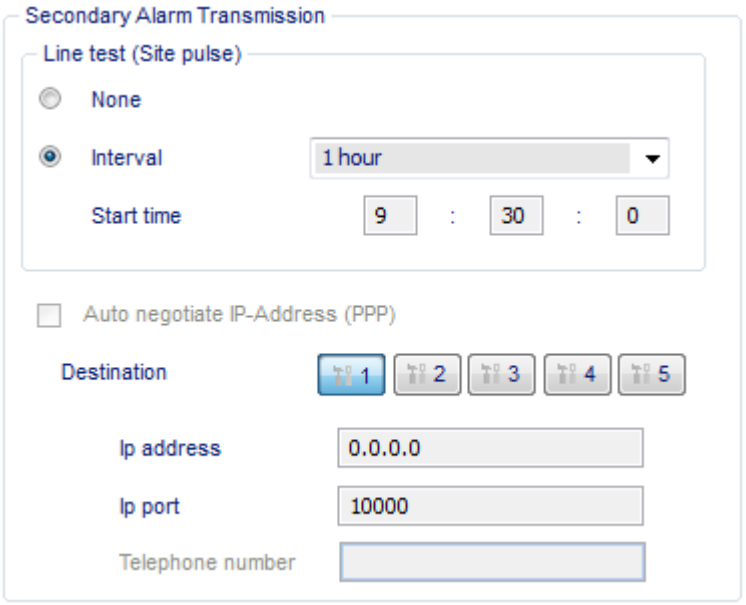
Parameter	Description	Default value
General: CMS ID	Sender signature (this number has to match the number programmed in the alarm management software)	3141593
General: FastTrace 2 Unit ID	Site identification number (number from 1 to 9999). This number has to be unique for each video system that sends alarms to the same computer.	1
General: Site name	Name of the site. This information is required if connecting to Central Video software. The site name can also be displayed on the camera images.	Site name
General: Connection timeout	Disconnects automatically if no more data is exchanged for the specified time duration.	3 (seconds)
General: Holdtime	This specifies a delay, expressed in seconds, before re-attempting to connect, when a connection error occurred. If “0”, the system will not try again (= only recommended if a backup connection is available).	600 (seconds)

8.1.2 Primary alarm transmission settings



Parameter	Description	Default value
Line test	○ None; ○ Interval: this will send a life check message every x minutes. Also set the time on which the first alarm transmission should be sent. ***Warning***: for dial-up networks it is recommended to execute the line test less frequent, because of the connection cost (e.g. 1 test a day).	None
auto-negotiate IP address (PPP)	This option is only available for a dial-up network. When ticked, IP addresses will be assigned by the CMS, during the time of the communication. This option is required if the CMS uses the Video Central Platinum software.	unticked
Destination	You can enter the parameters for 5 different computers that will receive alarms. Click the number you would like to define (or see). *Alarm reception requires appropriate alarm management software on the computer (e.g. M3000).*	
IP address	Enter the IP address of the computer that will receive alarms.	0.0.0.0
IP port	Enter the IP port on which alarms must be transmitted.	10000
Telephone number	Enter the telephone number to which alarms must be transmitted. This option is only available for a dial-up network.	-

8.1.3 Secondary alarm transmission settings



Parameter	Description	Default value
Line test	○ None; ○ Interval: this will send a life check message every x minutes. Also set the time on which the first alarm transmission should be sent. ***Warning***: for dial-up networks it is recommended to execute the line test less frequent, because of the connection cost (e.g. 1 test a day).	None
auto-negotiate IP address (PPP)	This option is only available for a dial-up network. When ticked, IP addresses will be assigned by the CMS, during the time of the communication. This option is required if the CMS uses the Video Central Platinum software.	unticked
Destination	You can enter the parameters for 5 different computers that will receive alarms. Click the number you would like to define (or see). *Alarm reception requires appropriate alarm management software on the computer (e.g. M3000).*	
IP address	Enter the IP address of the computer that will receive alarms.	0.0.0.0
IP port	Enter the IP port on which alarms must be transmitted.	10000
Telephone number	Enter the telephone number to which alarms must be transmitted. This option is only available for a dial-up network.	-

8.2 Arming/Disarming the video system

Events on the FastTrace 2 can be classified in the following groups:

- system messages: these are internal events (e.g. hard disk error, power supply fault, communication error, …);
- camera messages (e.g. video signal missing, contrast level too low, motion detected, …);
- network inputs: alarm inputs connected to external Net IO modules
- inputs: alarm inputs connected to the OTB IO card, accessible at the back of the video system;
- virtual inputs: events detected on interconnected S3100 security panels.
- workbits: calculated bits that provide alarm information. A combination of inputs can trigger a workbit.

Events have to be handled in a different way when the building is left unattended. Therefore, the building has to be armed. Arming can be done in three ways:

1) automatically according to a schedule;
2) manually, by a user who has to activate a switch;
3) by the CMS, executing the DN command line in TELNET (hint: type HE for syntax help).

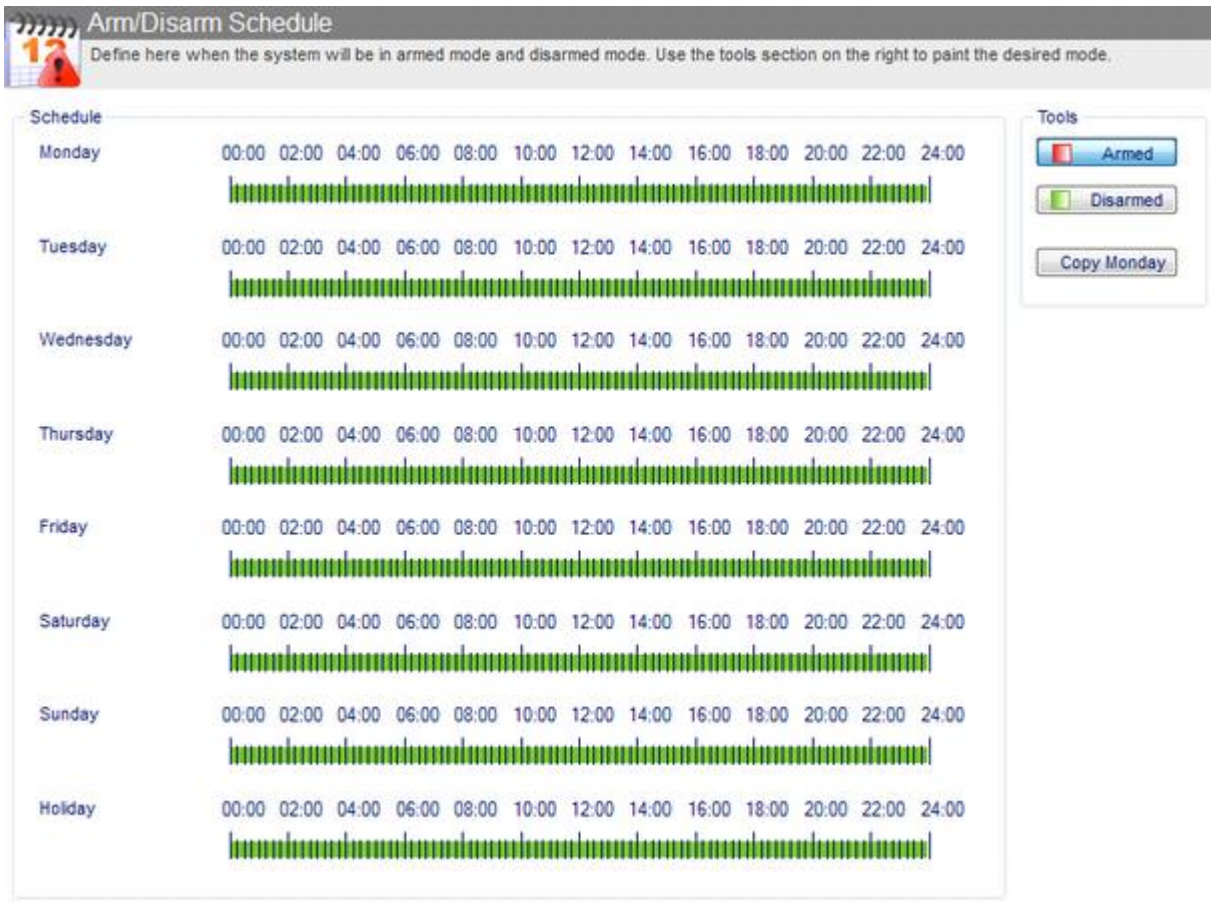
To define the behaviour of an alarm input during armed and disarmed state, modify the alarm profile that is assigned to this input.

Remark:

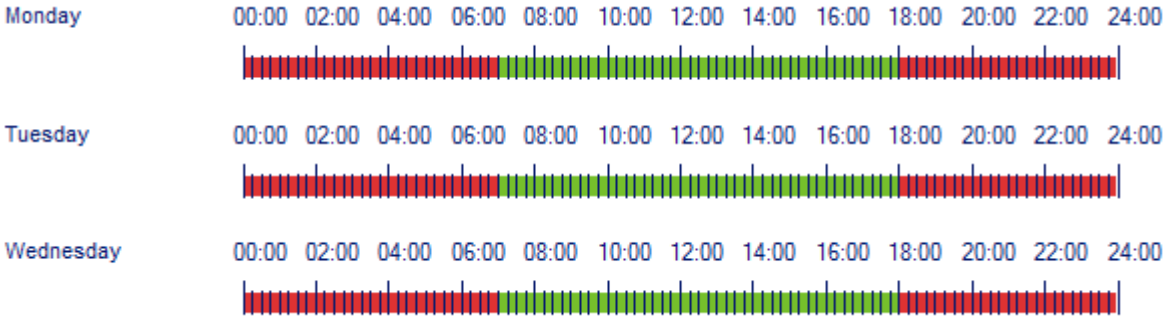
It is possible for other software developers to use the SDK (software development kit) in order to arm/disarm a building.

8.2.1 Arm/Disarm schedule

To insert a schedule to automatically arm/disarm a building, open **Settings > Behaviour > Arm/Disarm schedule**.



By default the system is always disarmed. To automatically arm the system for a given period, click ‘Armed’ in the *Tools* section and drag the mouse pointer over the desired period. The selected period will be indicated with a red bar.

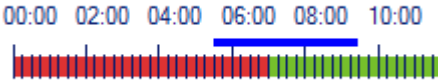


Click ‘Save’ to apply the new settings.

! The video system will be (dis)armed at the beginning of the programmed time zone. A switch can always force the system to another state.

Hint:

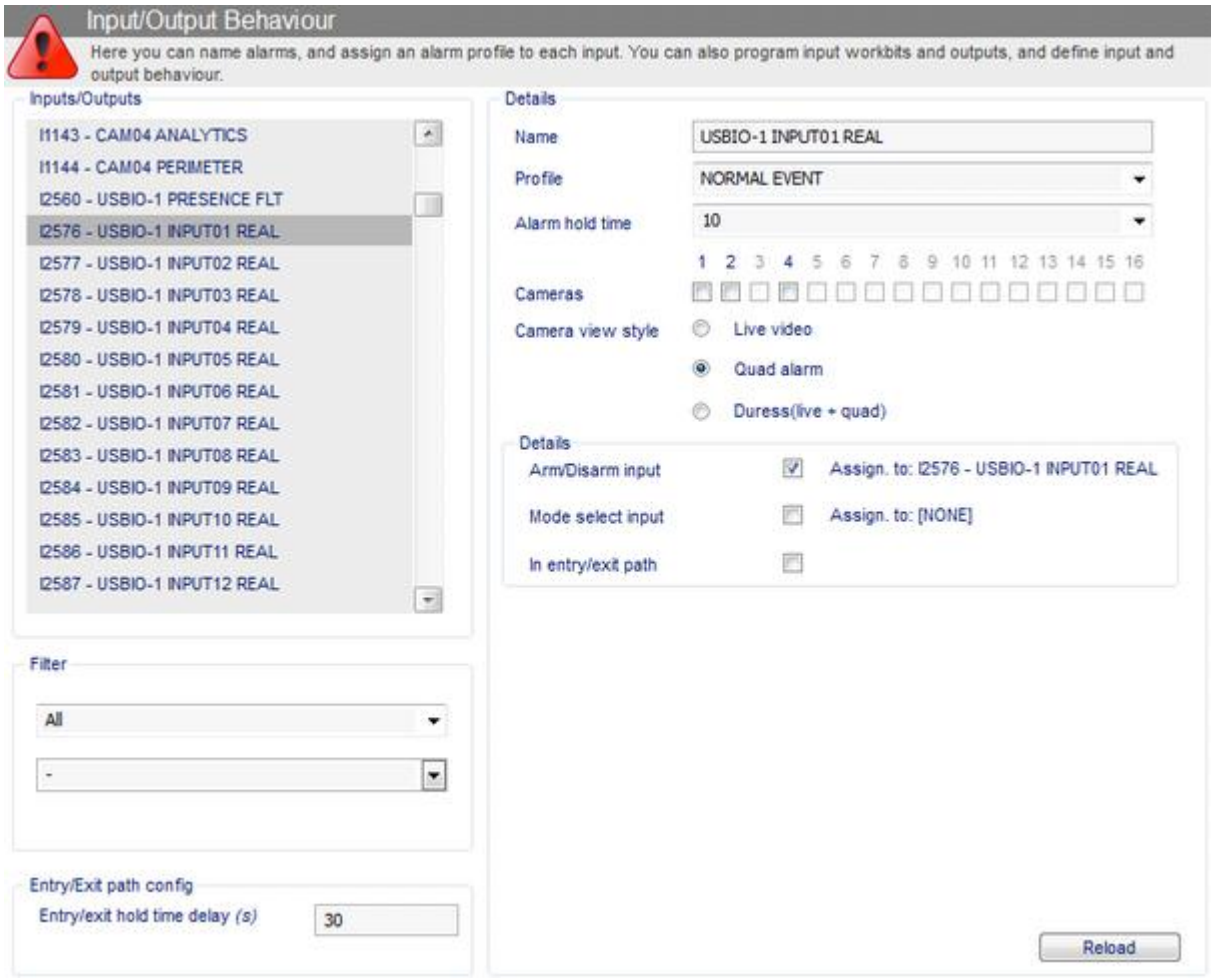
To zoom in on a part of the day, position the mouse pointer on the time scale, press the left mouse button and drag the mouse to the right (drawing a blue line). Release the mouse button.



To zoom out, position the mouse pointer on the time scale and click the right mouse button.

8.2.2 Arm/Disarm Switch

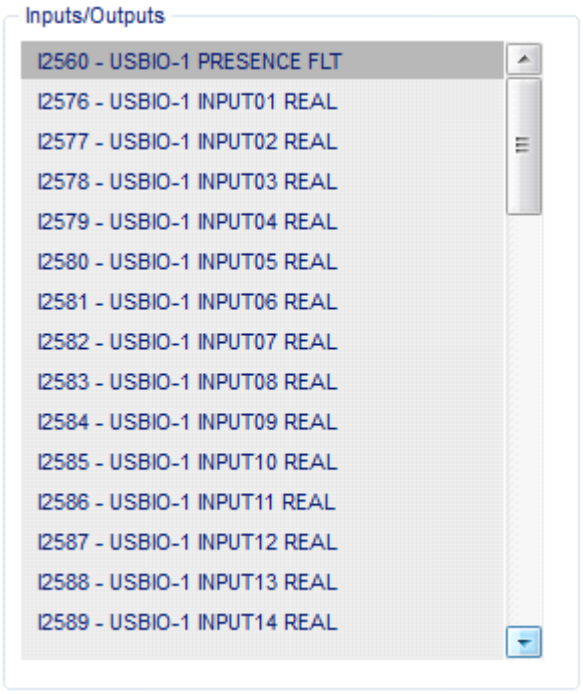
To define an arm/disarm switch, open **System > Behaviour > Input/output behaviour**. Select an input from the list. Mind: only real inputs (USB IO) or network inputs (Net IO) can be used. Apply a filter to reduce the list.


Input/Output Behaviour
Here you can name alarms, and assign an alarm profile to each input. You can also program input workbits and outputs, and define input and output behaviour.
Inputs/Outputs
I1143 - CAM04 ANALYTICS
I1144 - CAM04 PERIMETER
I2560 - USBIO-1 PRESENCE FLT
I2576 - USBIO-1 INPUT01 REAL
I2577 - USBIO-1 INPUT02 REAL
I2578 - USBIO-1 INPUT03 REAL
I2579 - USBIO-1 INPUT04 REAL
I2580 - USBIO-1 INPUT05 REAL
I2581 - USBIO-1 INPUT06 REAL
I2582 - USBIO-1 INPUT07 REAL
I2583 - USBIO-1 INPUT08 REAL
I2584 - USBIO-1 INPUT09 REAL
I2585 - USBIO-1 INPUT10 REAL
I2586 - USBIO-1 INPUT11 REAL
I2587 - USBIO-1 INPUT12 REAL
Filter
All
-
Entry/Exit path config
Entry/exit hold time delay (s)
30
Details
Name
USBIO-1 INPUT01 REAL
Profile
NORMAL EVENT
Alarm hold time
10
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Cameras
Camera view style
Live video
Quad alarm
Duress(live + quad)
Details
Arm/Disarm input
Assign. to: I2576 - USBIO-1 INPUT01 REAL
Mode select input
Assign. to: [NONE]
In entry/exit path
Reload

Tick the “Arm/Disarm” option; modify the settings if necessary and click ‘Save’ to apply the new settings.

8.3 Alarm inputs

To define alarm inputs, open **System > Behaviour > Input/Output behaviour**. Select an input from the list.

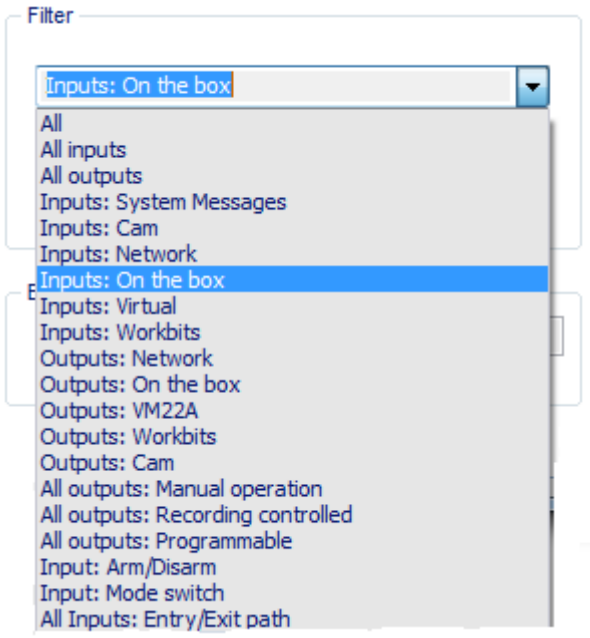

Inputs/Outputs
I2560 - USBIO-1 PRESENCE FLT
I2576 - USBIO-1 INPUT01 REAL
I2577 - USBIO-1 INPUT02 REAL
I2578 - USBIO-1 INPUT03 REAL
I2579 - USBIO-1 INPUT04 REAL
I2580 - USBIO-1 INPUT05 REAL
I2581 - USBIO-1 INPUT06 REAL
I2582 - USBIO-1 INPUT07 REAL
I2583 - USBIO-1 INPUT08 REAL
I2584 - USBIO-1 INPUT09 REAL
I2585 - USBIO-1 INPUT10 REAL
I2586 - USBIO-1 INPUT11 REAL
I2587 - USBIO-1 INPUT12 REAL
I2588 - USBIO-1 INPUT13 REAL
I2589 - USBIO-1 INPUT14 REAL

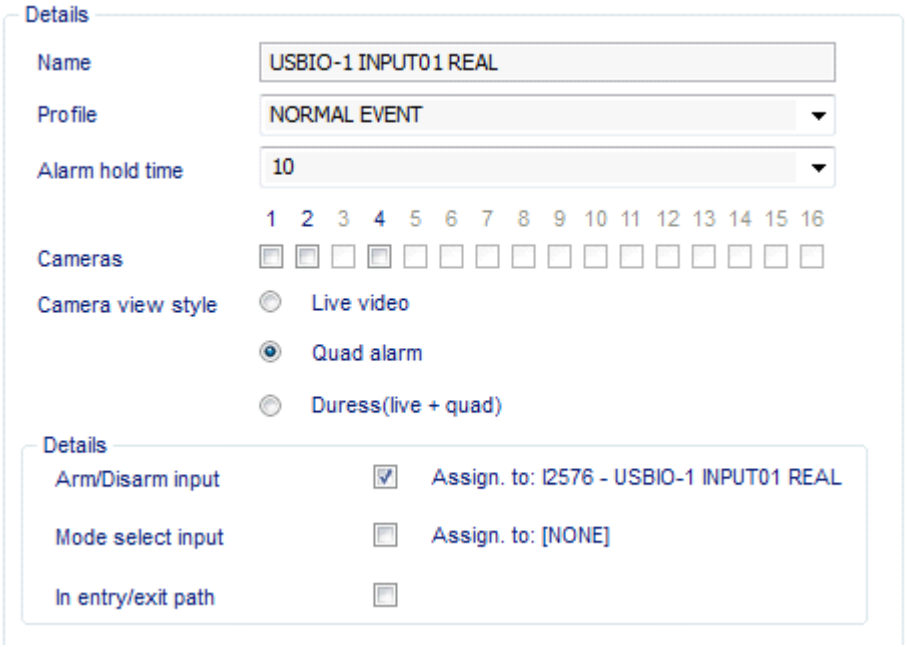
The input has to belong to one of these groups:

- **On the box:**
  inputs and outputs on the OTB IO cards, with alarm and tamper state; 20 inputs on the first set (= Main IO and Extension IO card), 20 inputs on the second set (Main IO and Extension IO card).
- **Network:**
  inputs and outputs on Net IO modules, connected to the Ethernet (local network).
- **System messages:**
  internal events and states, such as hard disk error, modem error, …
- **Cam:**
  camera alarms, including “no video alarm”, “contrast error” and “motion alarm”.
- **Virtual:**
  events detected on the interconnected S3100 alarm panel. Virtual inputs are selected by alarm profile (e.g. input activated upon motion on camera 1 or alarm on input 2 of the I/O card).
  (*see FCU Configurator for details*)
- **Arm/Disarm:**
  all inputs that have been programmed for arming/disarming
- **Mode Switch:**
  all inputs that have been programmed for mode switching.
- **Entry/Exit path:**
  all inputs that have been programmed within the entry/exit path (delayed events).
- **Workbits**:
  calculated bits that provide alarm information. A combination of inputs can trigger a workbit.

Hint:

Since the number of inputs and outputs is very long, it might be easier to find the desired input by limiting the list. To limit the list you can use the filter function:





Parameter	Description
Name	Enter a name (max 20 characters) to describe the alarm. It is recommended to use a description that is meaningful and relevant.
Profile	Select an alarm profile. This alarm profile defines the behaviour of the input.
Alarm Hold time	This sets the minimum time of activation of the alarm (in seconds). End-of-alarm will only be detected after this delay. This parameter will suppress a flow of events caused by a rattling alarm contact.
Cameras	Tick the desired cameras. Choose cameras that might reveal important information about the event.

Camera view style	Select the video information that should be available to the CMS. ○ Live video: the CMS can open a connection with the site to watch live images on the relevant cameras; ○ Quad: the CMS can retrieve pictures from the video system (3 stills are stored on the video system, taken from the relevant camera, with an adjustable interval); ○ Duress: both live images and pictures are available.

☞ To adjust the time between successive pictures, open **System > Connections > Video** and modify the parameter *Quad image interval*. The value is expressed in seconds. Mind: this parameter applies to all cameras!

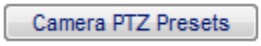
Arm/Disarm input	Tick this option if the input is used to arm and disarm the system.
Mode selection input	Tick this option if the input is used to switch the video system to a defined operation mode (mode 1 or mode 2). The mode of operation affects the behaviour of video recording!
Input in entry/exit path (value in seconds)	Tick this option if the alarm has to be delayed. The delay is specified by the parameter '*Entry/Exit hold time delay'*. On entry to the building, the video system has to be disarmed within this time to avoid alarms on the delayed inputs. On exit, the building has to be abandoned within this time counting from the moment when it is armed.

Modify the alarm parameters of the selected input and click **Save** to apply the new settings.

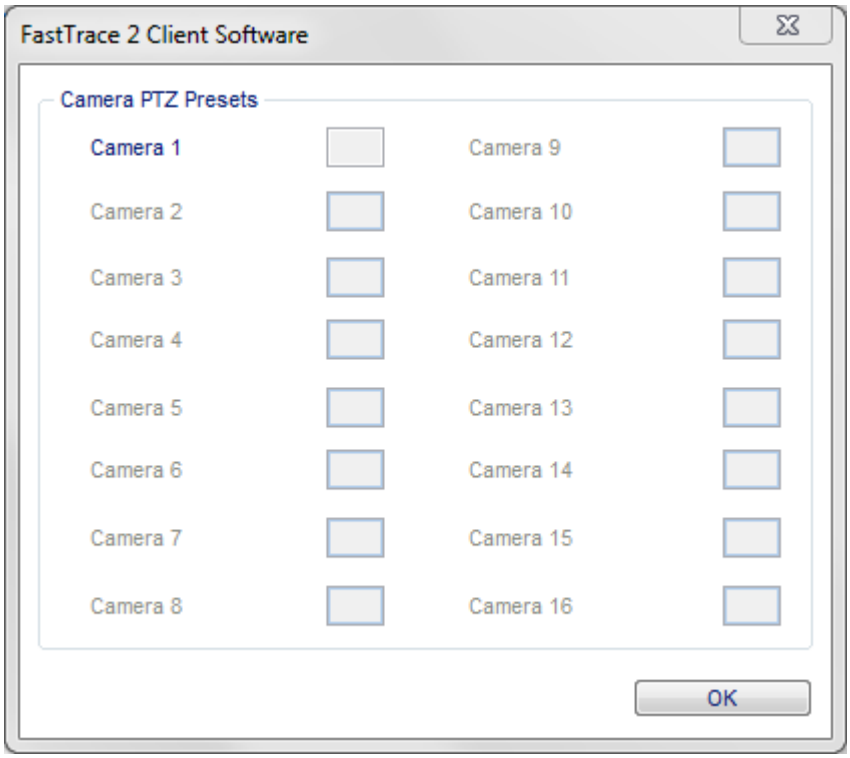
8.3.1 PTZ via I/O

It is possible to define PTZ preset positions via an input. Open the *Input/Output behaviour* window via **System > Behaviour > Input/Output behaviour**.

Select the desired input and click on Camera PTZ Presets.



You will get the following popup window:



All PTZ cameras can be provided with 1 specific PTZ preset. When an input is triggered, the camera will move to the configured PTZ preset position. The alarm message will be delayed, however, until the PTZ preset positioning time has expired. This is done to make sure no blurry images are recorded.

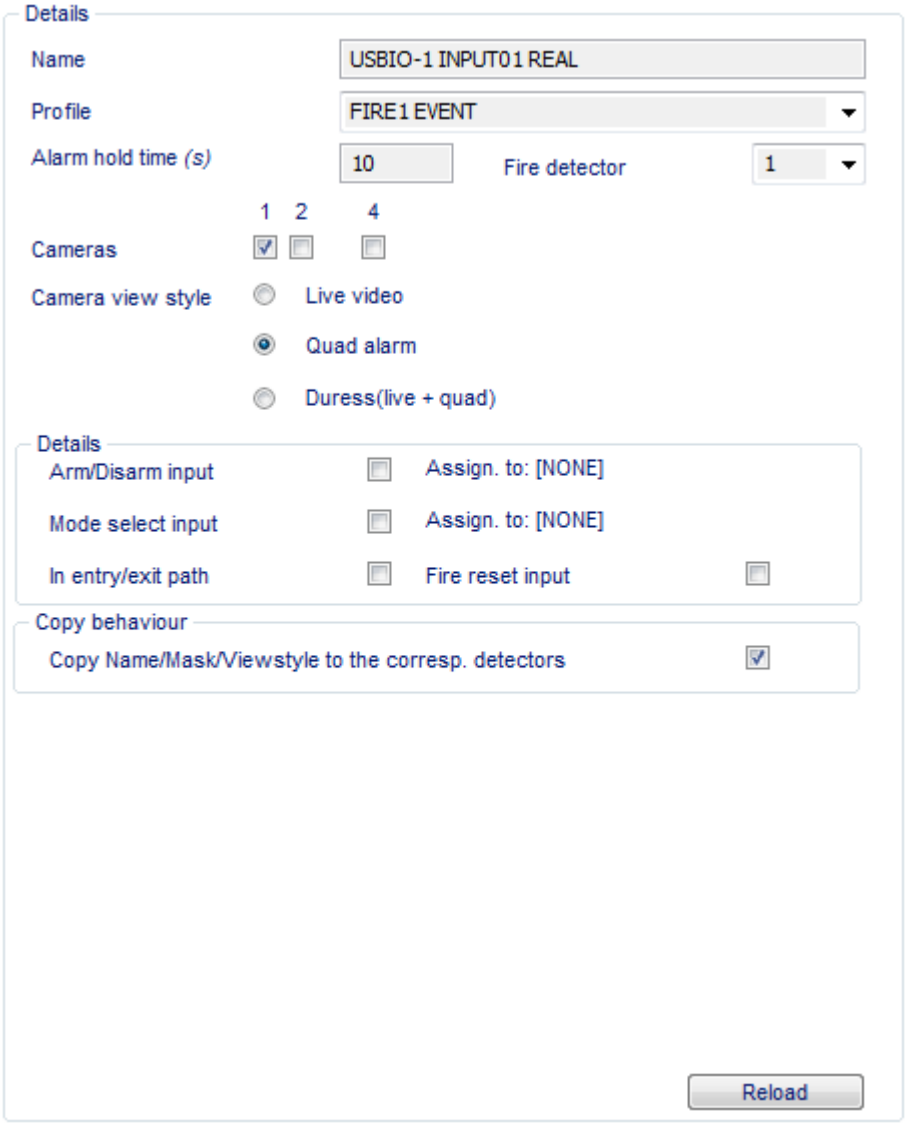
Mind:

It is not possible to define camera PTZ presets for system inputs.

8.3.2 Connecting fire detectors

You can connect up to 20 fire detectors to the FastTrace 2 server. These detectors can only be connected to real inputs on the FastTrace 2 server.

Open the *Input/Output behaviour* window via **System > Behaviour > Input/Output Behaviour**. Choose a fire event profile and attribute a fire detector number.

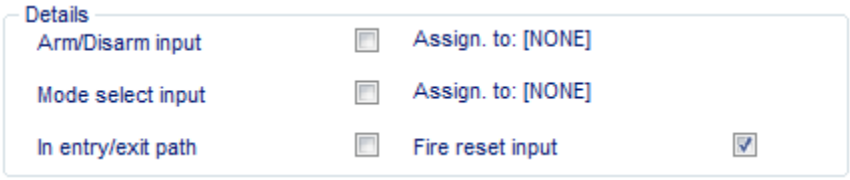


You can tick the option – by default this option is ticked already – Copy Name/Mask/Viewstyle to the corresponding detectors to make sure that all modifications are automatically copied to the corresponding detectors.

How many inputs from the same detector you can configure, depends on the type of the fire detector. Please consult the technical documentation of the specific detector for more information.

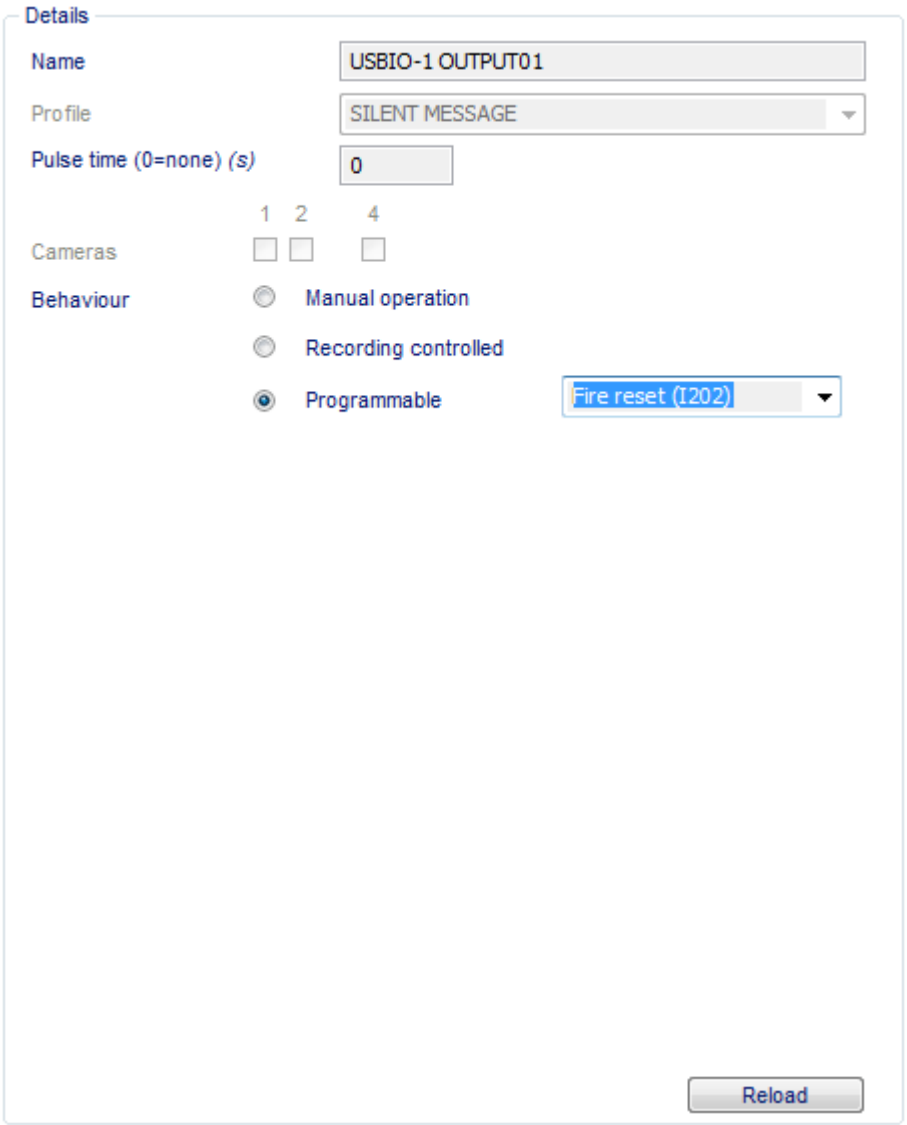
8.3.2.1 Fire reset input and output

You can configure an input as fire reset input. This means that when this input is activated an output will be activated as a consequence. The output will reset all fire detectors.



To define the fire reset output, proceed as follows:

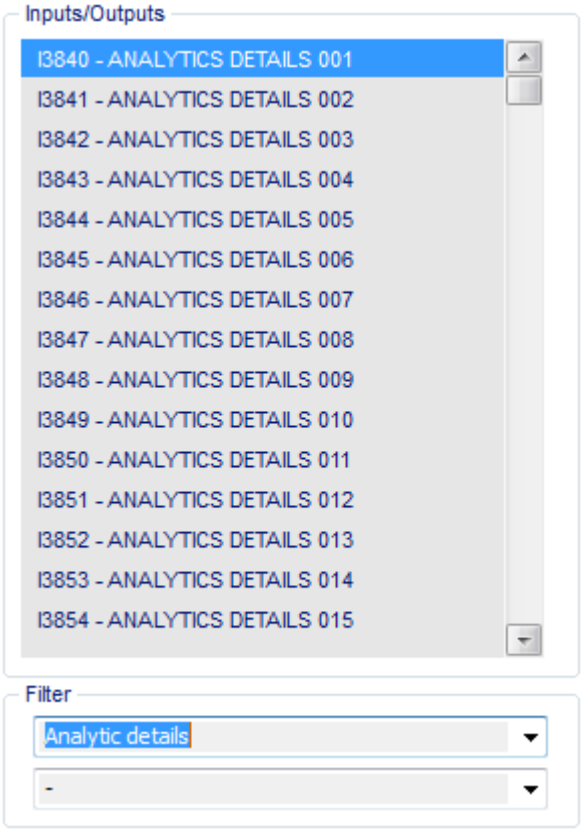
1. Select an output from the list.
2. In the *Details* section to the right, tick the option Programmable as Behaviour.
3. Choose the option Fire reset (I202) from the dropdown list.



To reset the fire detectors you can also use the command ***GR,fire*** (in TELNET or Hyperterminal).

8.3.3 IntrusionTrace alarms

For each camera a set of 16 extra alarms have been created to use with IntrusionTrace. These alarms provide extra information concerning the IntrusionTrace detection on a camera. The alarms can also be used for example to trigger PTZ cameras to zoom in on the detected area on an IntrusionTrace camera.


Inputs/Outputs
I3840 - ANALYTICS DETAILS 001
I3841 - ANALYTICS DETAILS 002
I3842 - ANALYTICS DETAILS 003
I3843 - ANALYTICS DETAILS 004
I3844 - ANALYTICS DETAILS 005
I3845 - ANALYTICS DETAILS 006
I3846 - ANALYTICS DETAILS 007
I3847 - ANALYTICS DETAILS 008
I3848 - ANALYTICS DETAILS 009
I3849 - ANALYTICS DETAILS 010
I3850 - ANALYTICS DETAILS 011
I3851 - ANALYTICS DETAILS 012
I3852 - ANALYTICS DETAILS 013
I3853 - ANALYTICS DETAILS 014
I3854 - ANALYTICS DETAILS 015
Filter
Analytic details
-

These alarms have been defined as IntrusionTrace alarms:

- Camera 1: I3840 through I3855
- Camera 2: I3856 through I3871
- Camera 3: I3872 through I3887
- Camera 4: I3888 through I3903
- Camera 5: I3904 through I3919
- Camera 6: I3920 through I3935
- Camera 7: I3936 through I3951
- Camera 8: I3952 through I3967
- Camera 9: I3968 through I3983
- Camera 10: I3984 through I3999
- Camera 11: I4000 through I4015
- Camera 12: I4016 through I4031
- Camera 13: I4032 through I4047
- Camera 14: I4048 through I4063
- Camera 15: I4064 through I4079
- Camera 16: I4080 through I4095

These alarms can be added to a detection area or a trigger line in the *IntrusionTrace Configuration* window.

8.4 Alarm profiles

8.4.1 The default profiles

By default the video system has been equipped with 12 standard alarm profiles:

- 1 – NORMAL EVENT
- 2 – PRIMARY EVENT
- 3 – BACKUP EVENT
- 4 – SILENT MESSAGE
- 5 – SINGLE EVENT
- 6 – ACTIVE SENSOR EVENT
- 7 – FIRE1 EVENT
- 8 – FIRE2 EVENT
- 9 – NON-FIRE ALARM
- 10 – FIRE ACTION
- 11 – FIRE ALERT
- 12 – FIRE TROUBLE

To modify the behaviour of alarm transmission of inputs, you need to modify the associated alarm profile of the input. It is however not recommended to modify the default alarm profiles. It's better to create a new alarm profile with different settings.

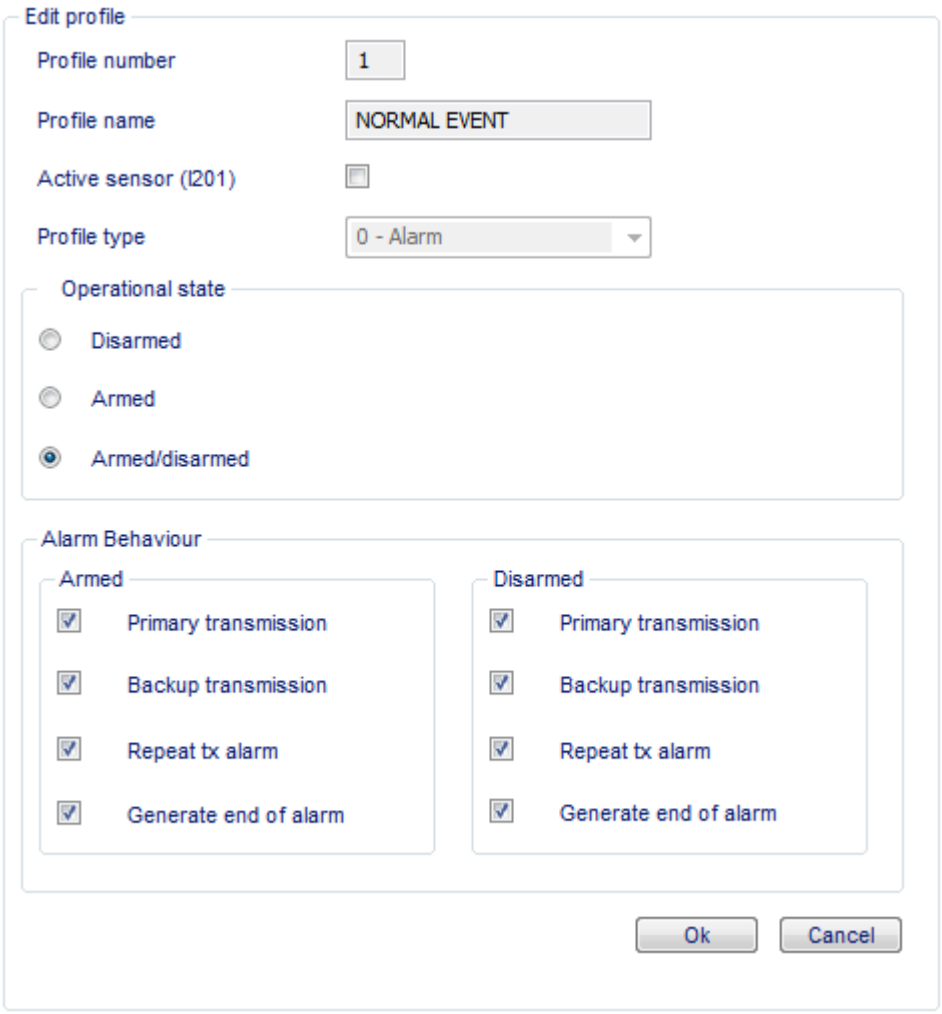
Open the *Alarm profiles* window via **System > Behaviour > Alarm profiles**.

Alarm Profiles
Each alarm is assigned a certain profile which defines how it must respond. Here you can define the different profiles.
Alarm Profiles
1 - NORMAL EVENT
2 - PRIMARY EVENT
3 - BACKUP EVENT
4 - SILENT MESSAGE
5 - SINGLE EVENT
6 - ACTIVE SENSOR EVENT
7 - FIRE1 EVENT
8 - FIRE2 EVENT
9 - NON-FIRE ALARM
Add
Edit
Remove

Select the desired alarm profile from the list and click **Edit**. To the right the *Edit profile* section appears.

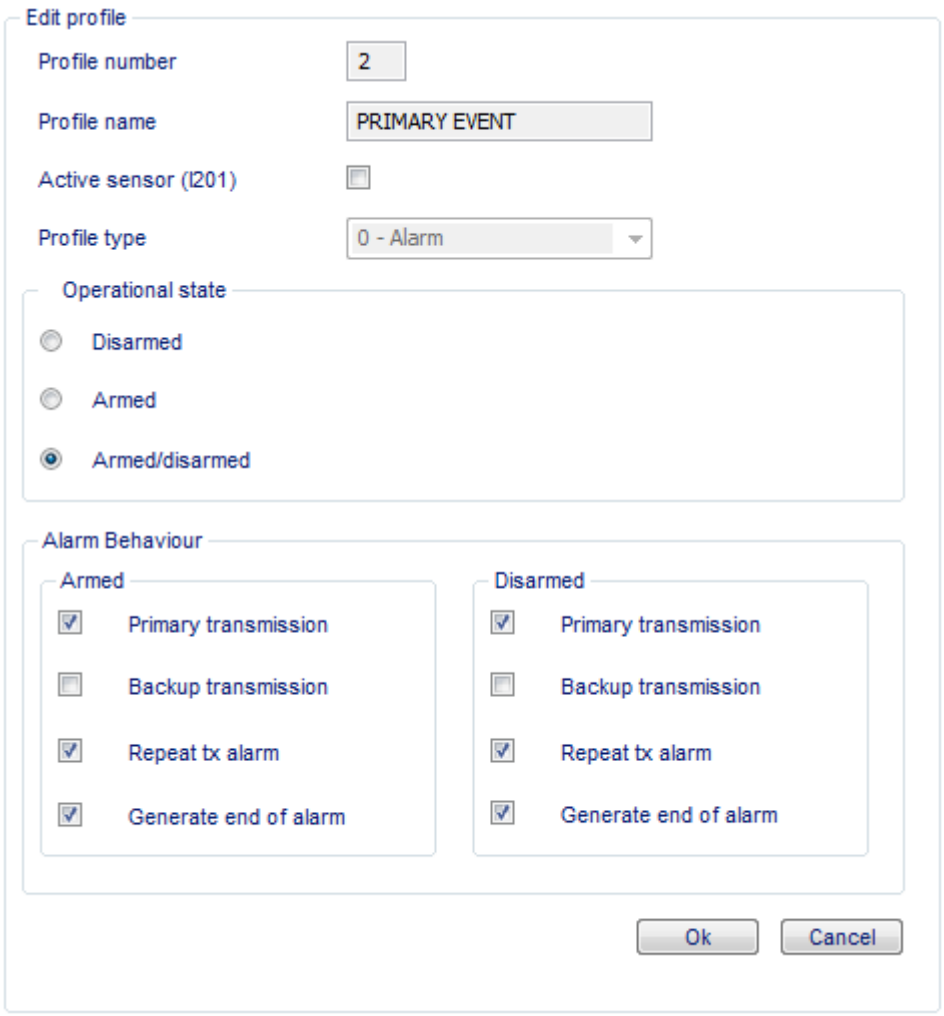
8.4.1.1 Normal event profile

A normal event profile is defined to send alarms for all detections to the primary and backup transmission destination. It also does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be send to indicate that the alarm is no longer sustained.



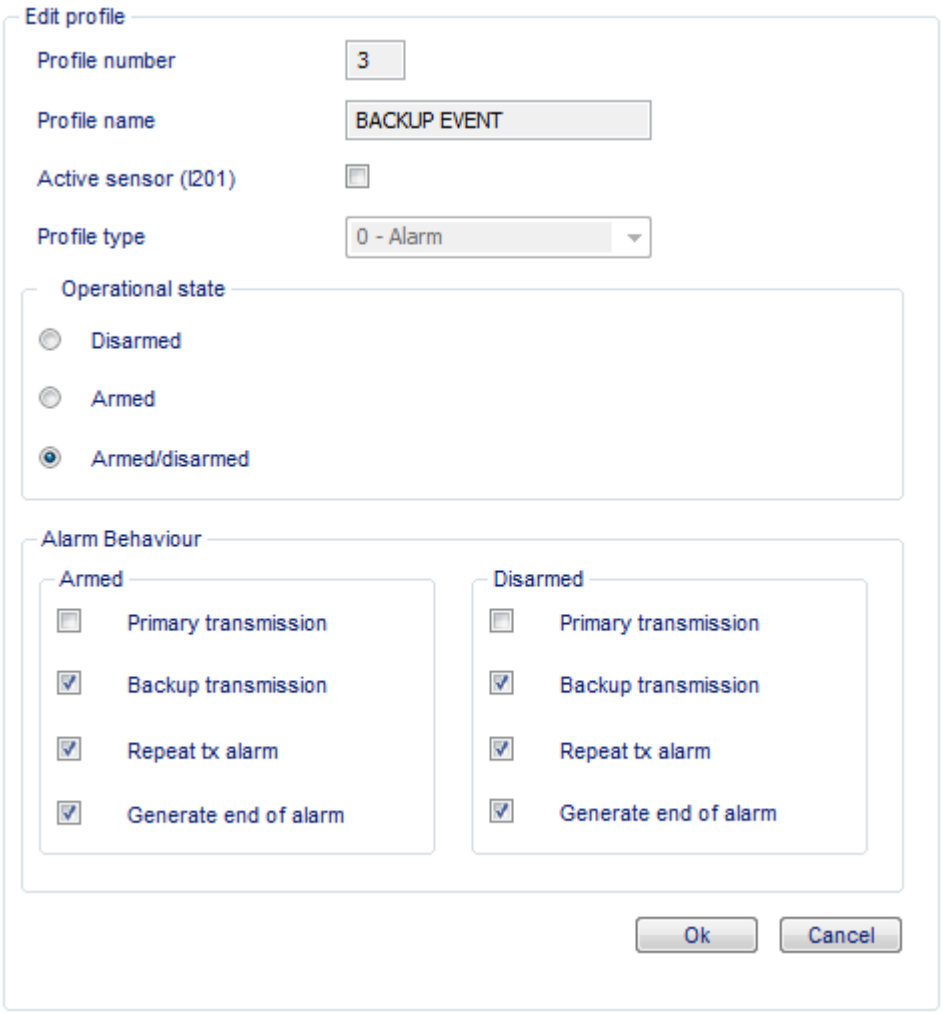
8.4.1.2 Primary event profile

A primary event profile is defined to send alarms for all detections to the primary transmission destination (and not to the backup transmission destination). It also does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be send to indicate that the alarm is no longer sustained.



8.4.1.3 Backup event profile

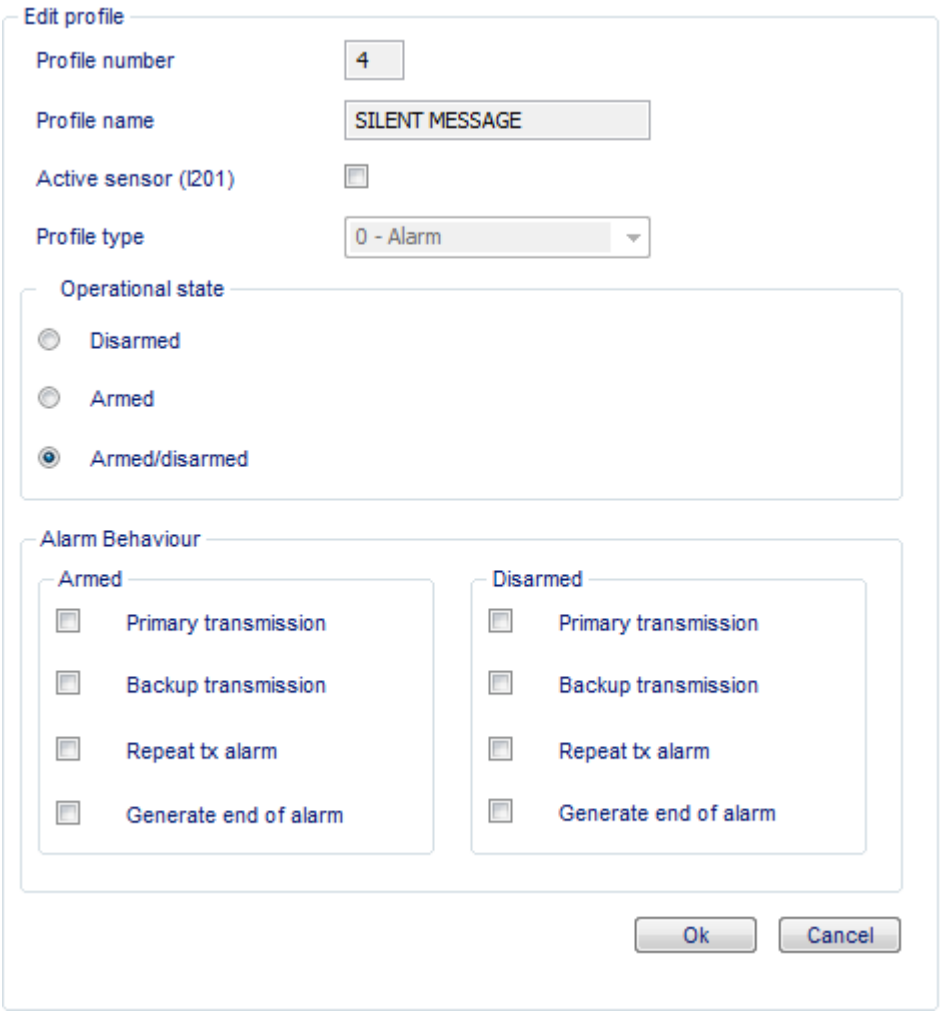
A backup event profile is defined to send alarms for all detections to the backup transmission destination (and not to the primary transmission destination). It also does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be send to indicate that the alarm is no longer sustained.



8.4.1.4 Silent message profile

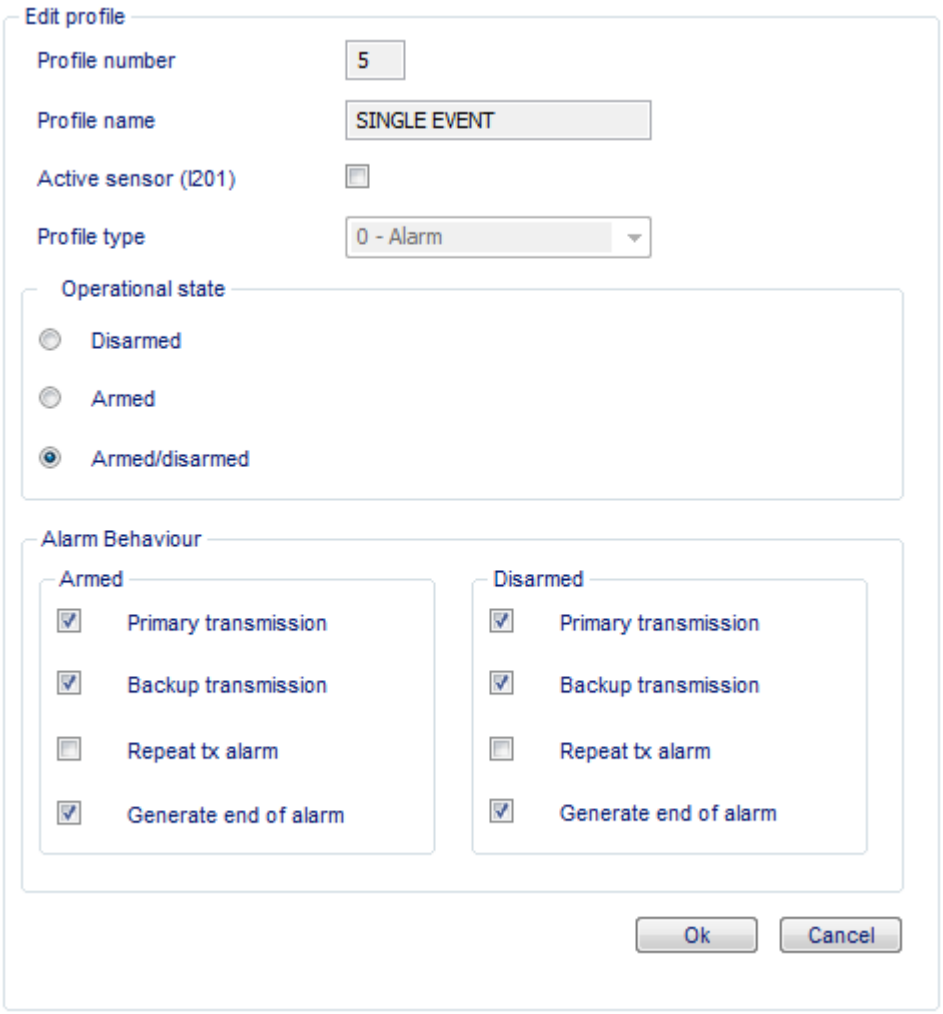
A silent message profile is defined to generate an alarm, but the alarm is not send to any transmission destination.

The alarm message is generated in both armed and disarmed state, but will not be sent to an alarm management system (like M3000). The idea behind this type of alarm is to get an overview in the log file.



8.4.1.5 Single event profile

A single event profile is defined to send alarms for all detections to the primary and backup transmission destination. It also does not take the operational state into account: the alarm will be generated in both armed and disarmed state. When the end of alarm is detected, a new alarm message will be send to indicate that the alarm is no longer sustained. The alarm will, however, not be repeated every 15 minutes as long as the alarm is sustained.

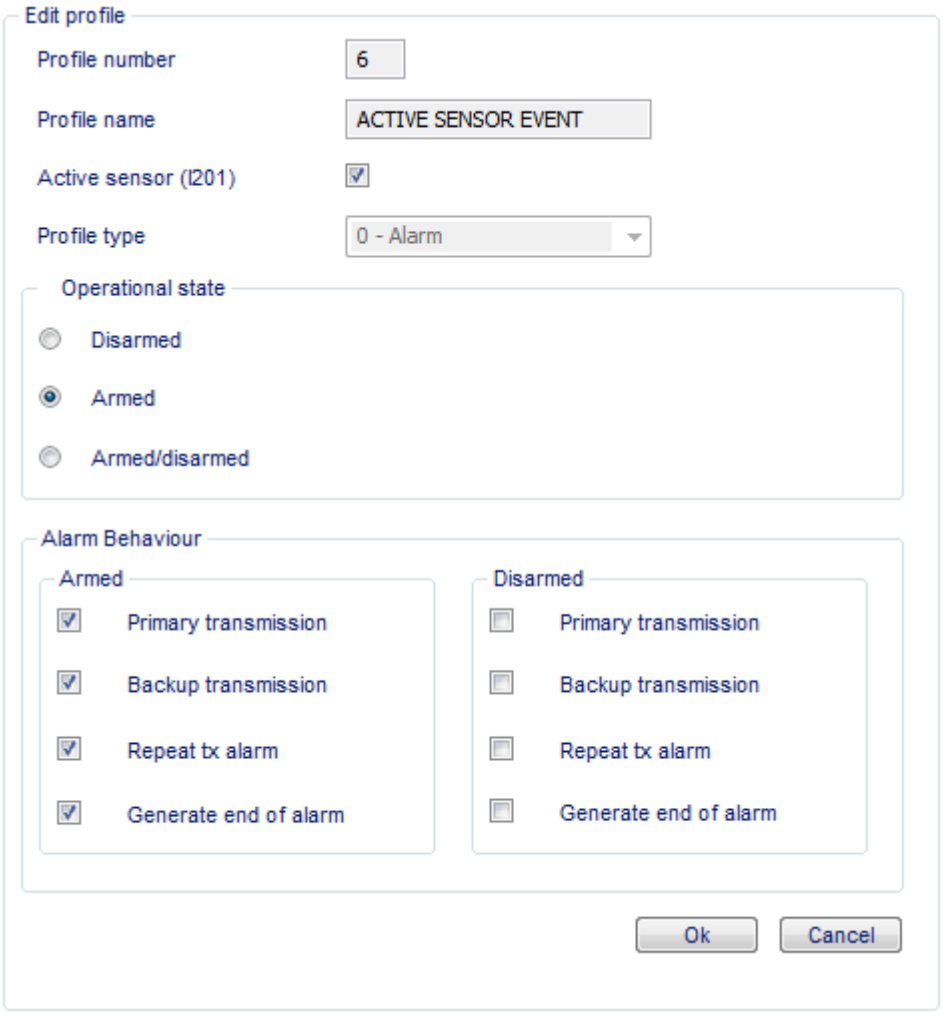


8.4.1.6 Active sensor event profile

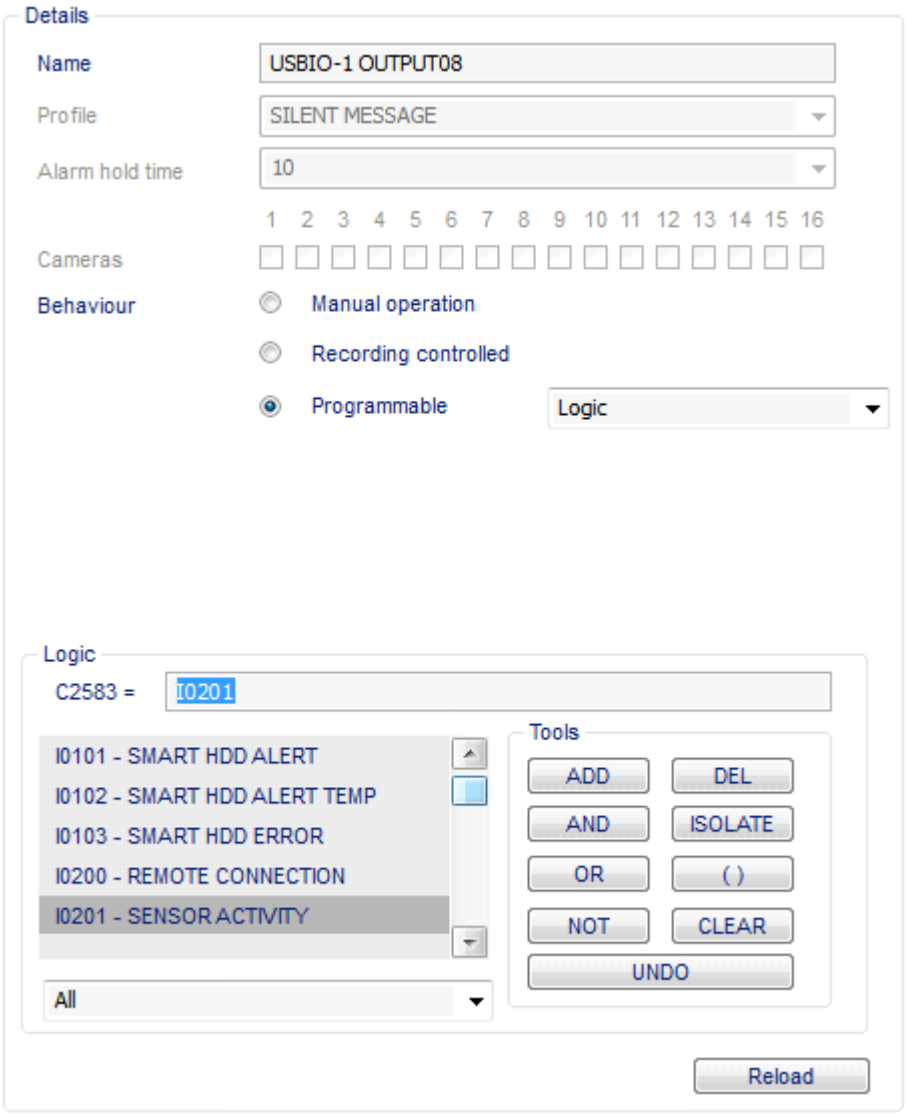
A normal event profile is defined to send alarms for all detections to the primary and backup transmission destination. This alarm is only generated when the operational state of the video system is set to armed.

This alarm profile also triggers input I201, thus activating the active sensor. Input I201 is used to inform the user that some sensors are still active. This will avoid arming the system while sensors are still in alarm.

Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be send to indicate that the alarm is no longer sustained.



To activate an output on input I201, open **System > Behaviour > Input/Output behaviour**, select an output (filter on *On the box* outputs to see only the physical outputs) and choose Programmable. Select I201 – Sensor Activity as input with Logics and click ‘Add’ under “Tools”.



All sensors assigned to an alarm profile that triggers I201, have to return to idle state in order to reset the selected output. When this condition is fulfilled, the user can arm the video system without triggering a false alarm.

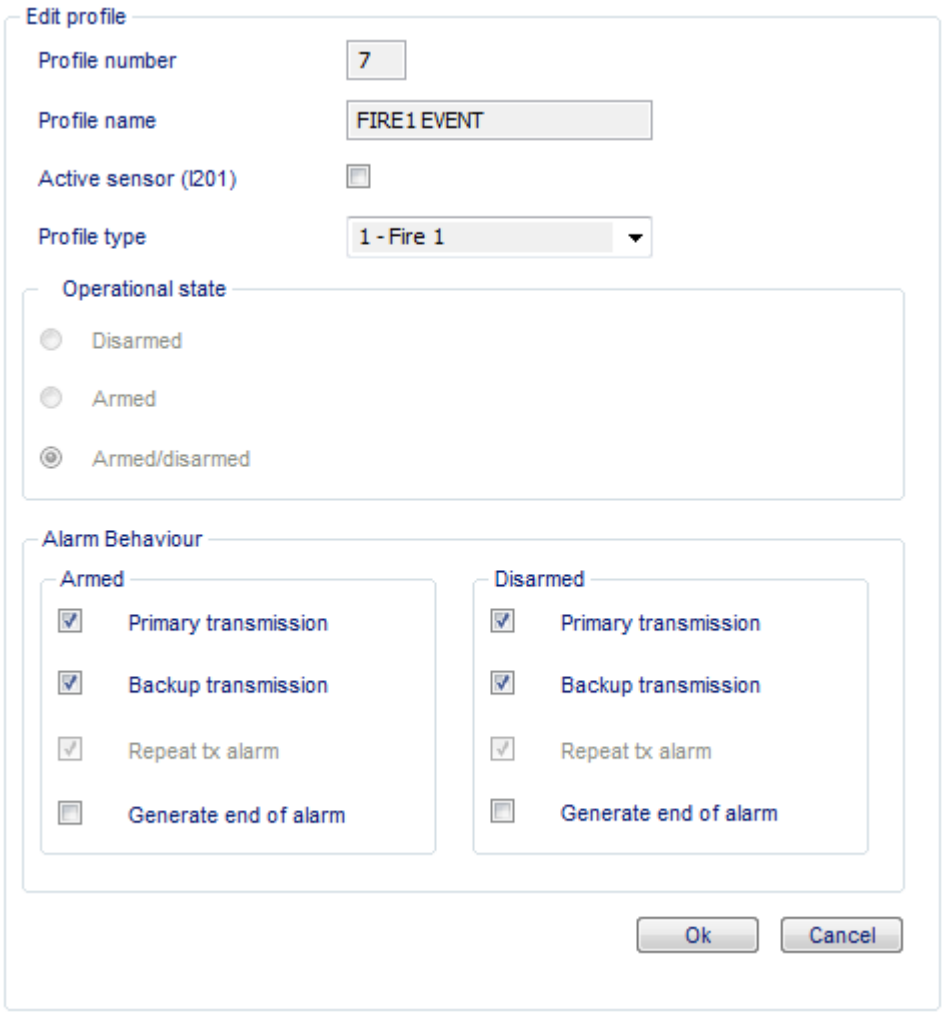
8.4.1.7 Fire1 event profile

The fire 1 event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For Fire 1 events the profile type is set to fire 1. This type indicates that a significant fire indication is present at the scene.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



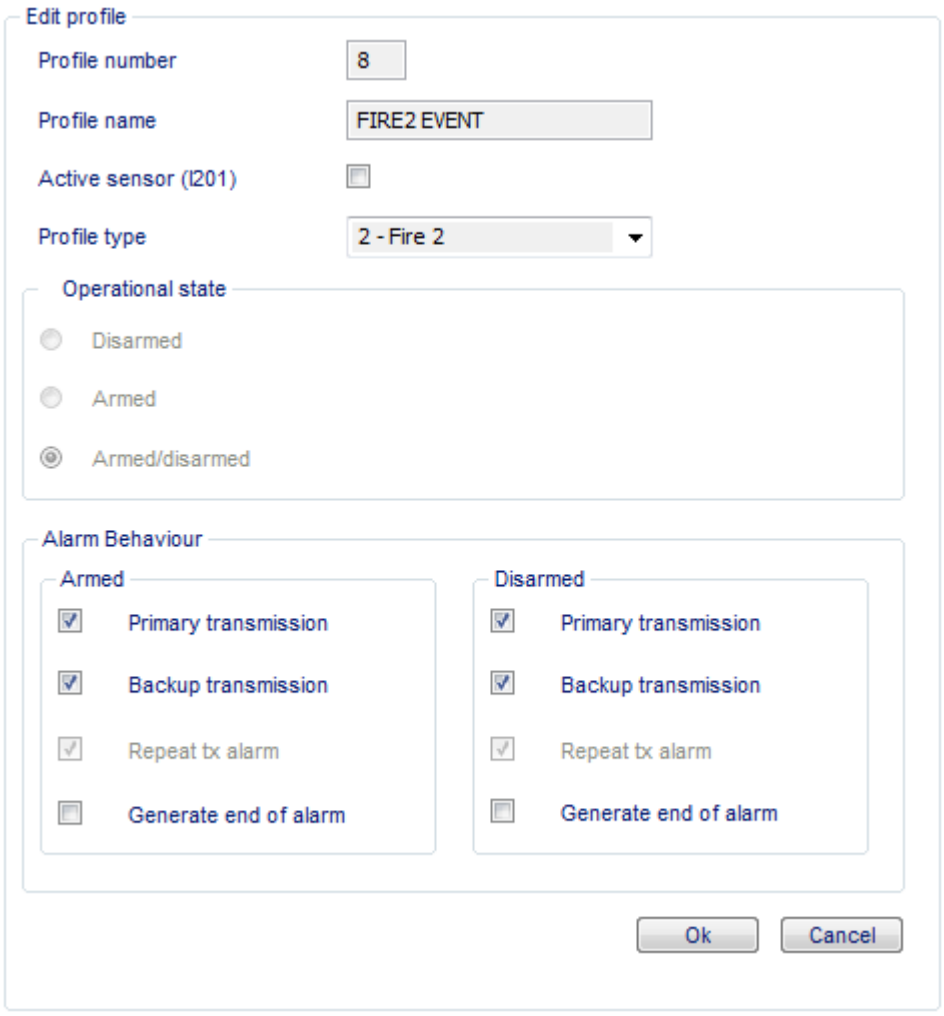
8.4.1.8 Fire2 event profile

The fire 2 event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For Fire 2 events the profile type is set to fire 2. This type indicates that fire is definitely present at the scene.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



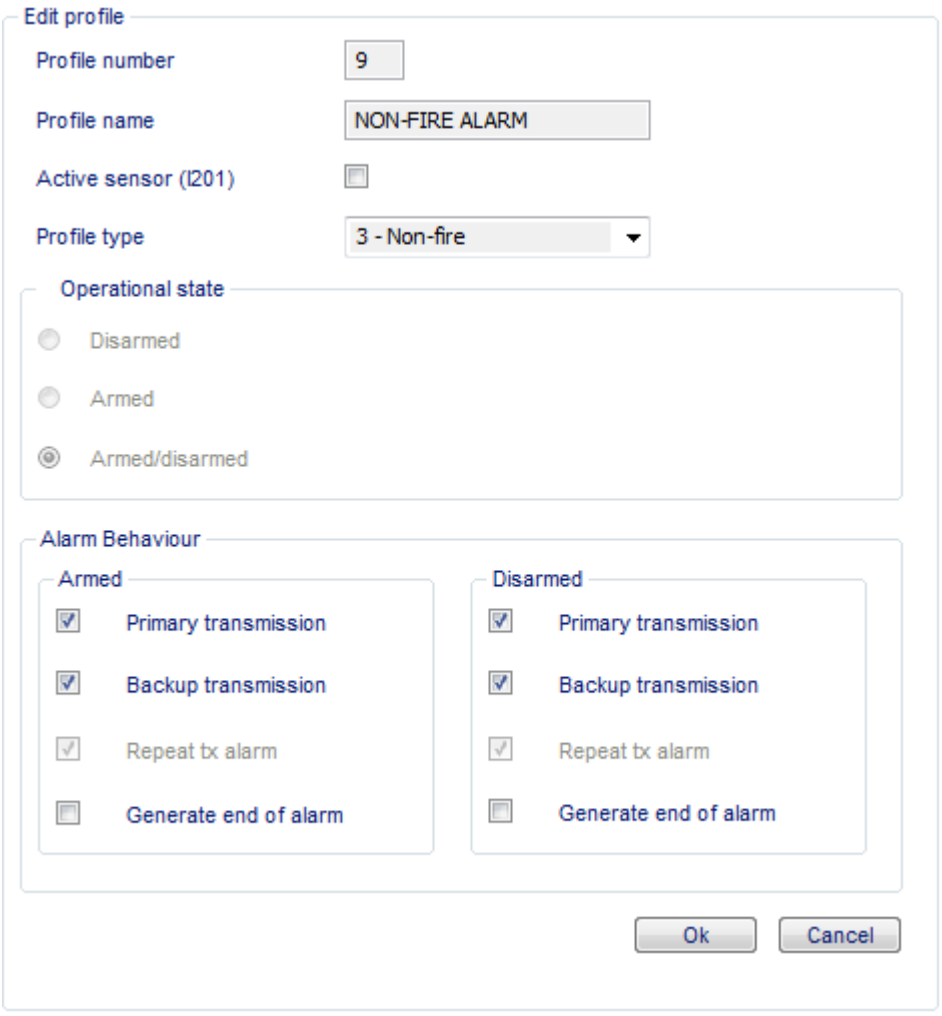
8.4.1.9 Non-fire alarm profile

The non-fire event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For non-fire events the profile type is set to non-fire. This type indicates that a non-fire event (e.g. a general purpose input on the sensor) is present at the scene.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



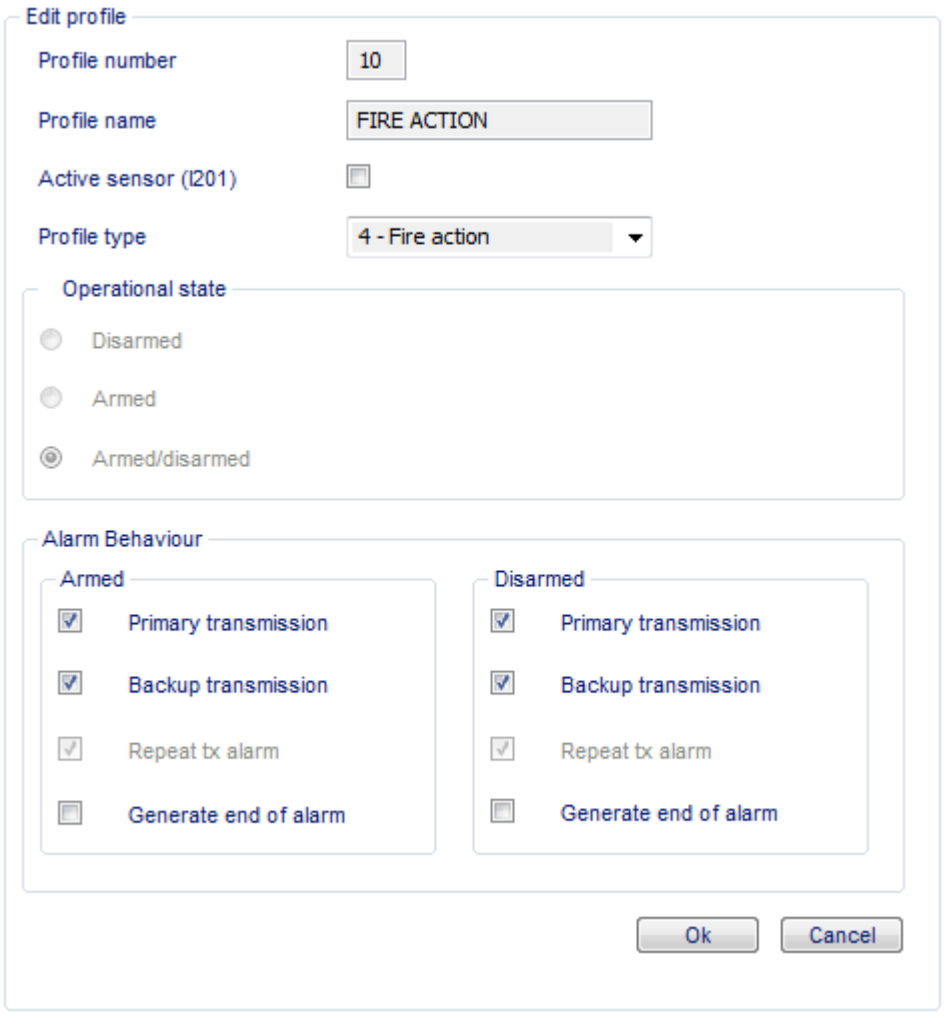
8.4.1.10 Fire action profile

The fire action event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For fire action events the profile type is set to fire action. This type indicates that there are indications of fire at the scene and that investigation is needed.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



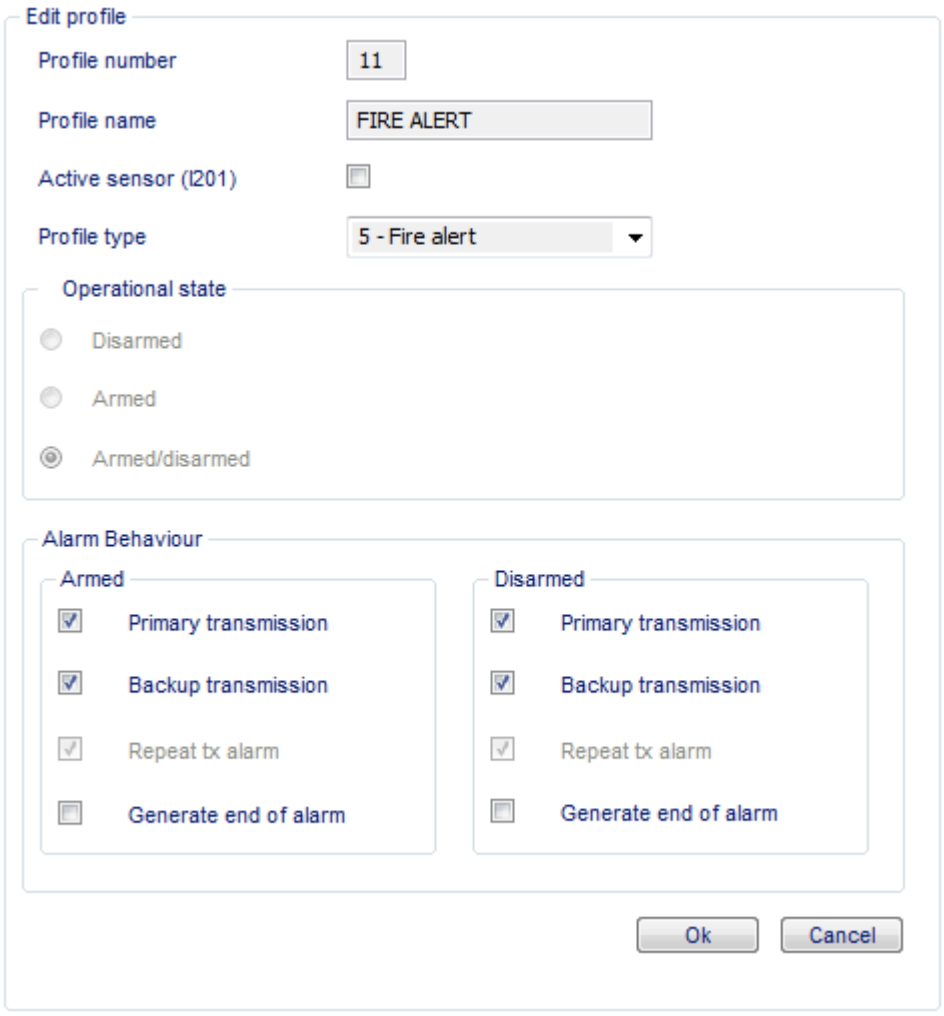
8.4.1.11 Fire alert profile

The fire alert event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For fire alert events the profile type is set to fire alert. This type indicates that there is a fire indication at the scene that is higher than the background level.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



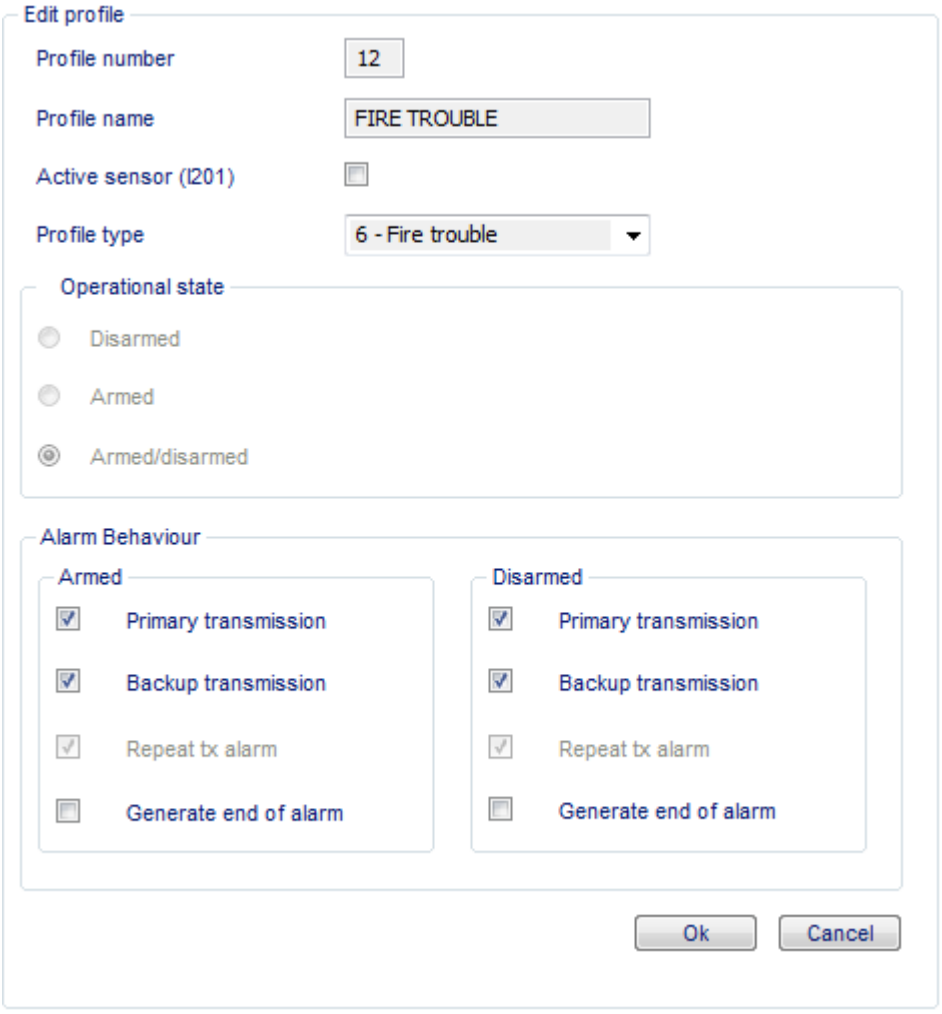
8.4.1.12 Fire trouble profile

The fire trouble event profile is designed to send alarm messages to both primary and backup transmission destinations in case of fire detection.

With fire events you can choose the profile type. For fire trouble events the profile type is set to fire trouble. This type indicates that there is a fault with a component of the system.

Each fire alarm profile is set to send alarms in both armed and disarmed state. The only way to modify this is by unticking the options in the *Alarm Behaviour* section.

Every fire alarm will be repeated until the alarm is no longer sustained. The fire alarm message will be resent every 15 minutes.



8.4.2 Adding a new profile

If not all numbers have been used, you can also add a new alarm profile. Up to 32 alarm profiles can be stored.

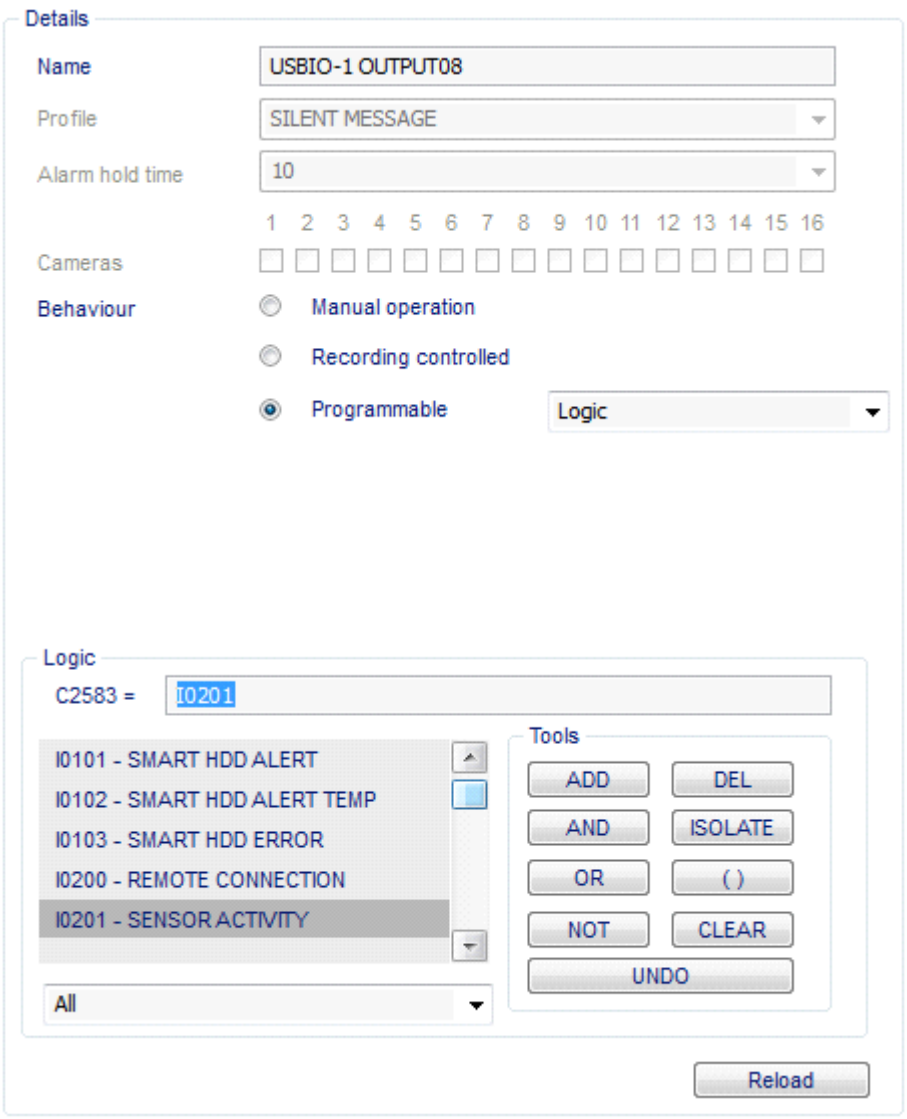
Click ‘Add’ to create a new alarm profile and enter all necessary parameters. Click ‘Remove’ to delete the selected alarm profile. Mind: you cannot delete an alarm profile that has been attributed.

Parameter	**Description**
Profile name	Enter a description (max 20 characters) for the alarm profile. It is recommended to use a meaningful and relevant description.
Active sensor output	If ticked, input I201 – if active – will be triggered. Input I201 can be used to inform the user that some sensors are still active. This will avoid arming the system while sensors are still in alarm. (see hint underneath)
Operational state	O Disarmed: inputs are only monitored when the system is disarmed; O Armed: inputs are only monitored when the system is armed; O Armed/disarmed: inputs are always monitored.
Alarm Transmission Behaviour	❑ Primary transmission: send events to the CMS via the main connection; ❑ Backup transmission: send events to the CMS via the backup connection (if available). The backup connection will only be used if transmission on the main connection has failed! ❑ Repeat tx alarm: send reminders at regular times (each 15 minutes) if alarm is sustained; ❑ Generate end of alarm: send message to CMS when input returns to normal state.

Click ‘Save’ to apply the new settings.

Hint:

To activate an output on input I201, open **System > Behaviour > Input/Output behaviour**, select an output (filter on *On the box* outputs to see only the physical outputs) and choose Programmable. Select *I201 – Sensor Activity* as input with *Logics* and click **Add** under *Tools*.

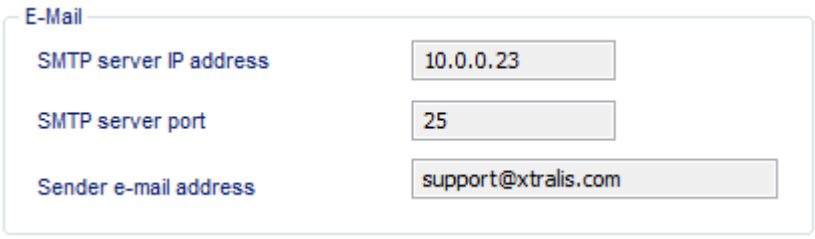


All sensors assigned to an alarm profile that triggers I201, have to return to idle state in order to reset the selected output. When this condition is fulfilled, the user can arm the video system without triggering a false alarm.

8.5 Email server settings

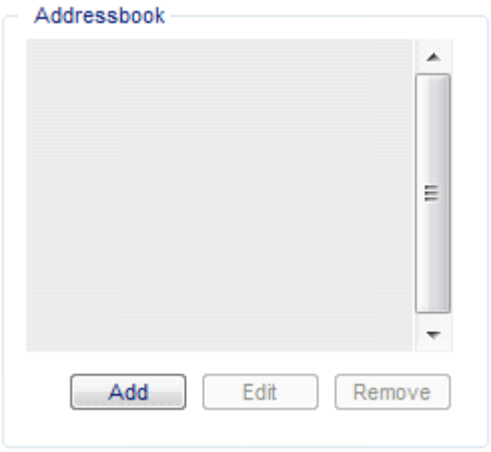
If the video system needs to send an email to specific recipients when detecting a specific event, the email SMTP server and email sender address need to be inserted. Mind: the email address of the email sender may need to be an existing email account, depending on the SMTP server settings.

Open the Email window via **System > Connections > Email**.

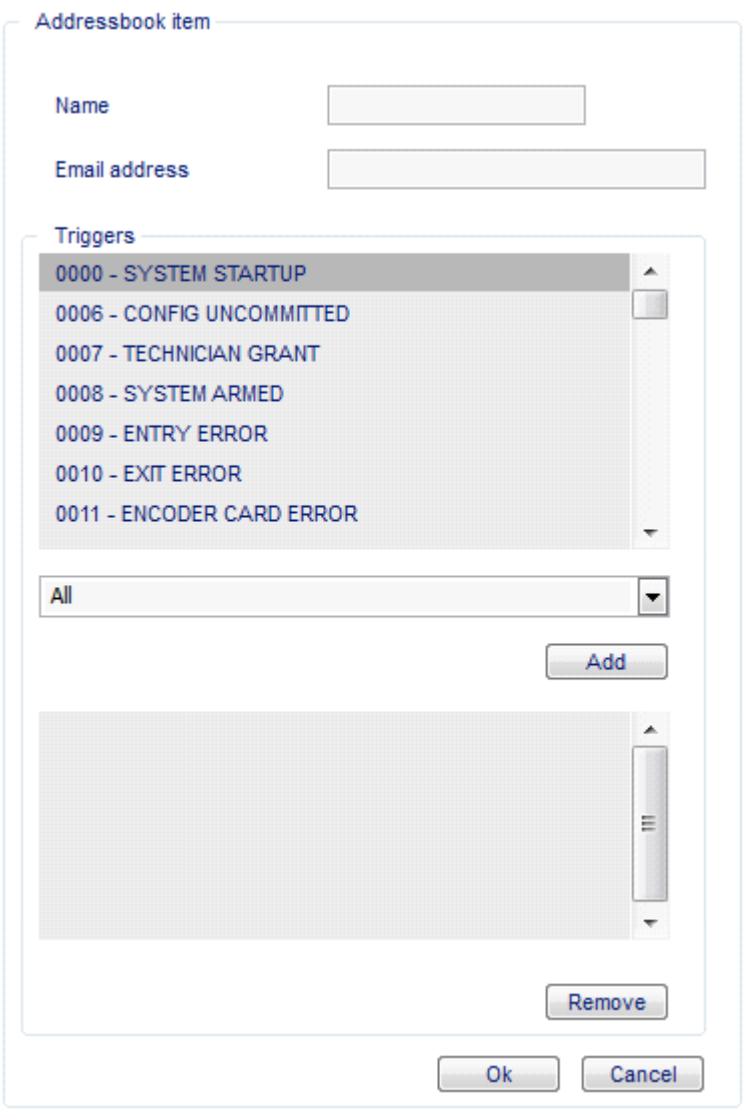


8.5.1 Email address book

Open the address book window via **System > Behaviour > Email Addressbook**. Click ‘Add’ to add a new contact.



A new section will appear to the right.



Enter the name and email address of the recipient.

Select the different notifications that you want to send to this recipient. You can add selections by selecting a trigger and clicking ‘Add’.

You can also delete a trigger from the list. Select the desired trigger in the list and click ‘Delete’. This will only delete the trigger from the recipient’s list of triggers, and not the trigger itself.

Click ‘OK’ and ‘Save’ to apply the new settings.

Remark:

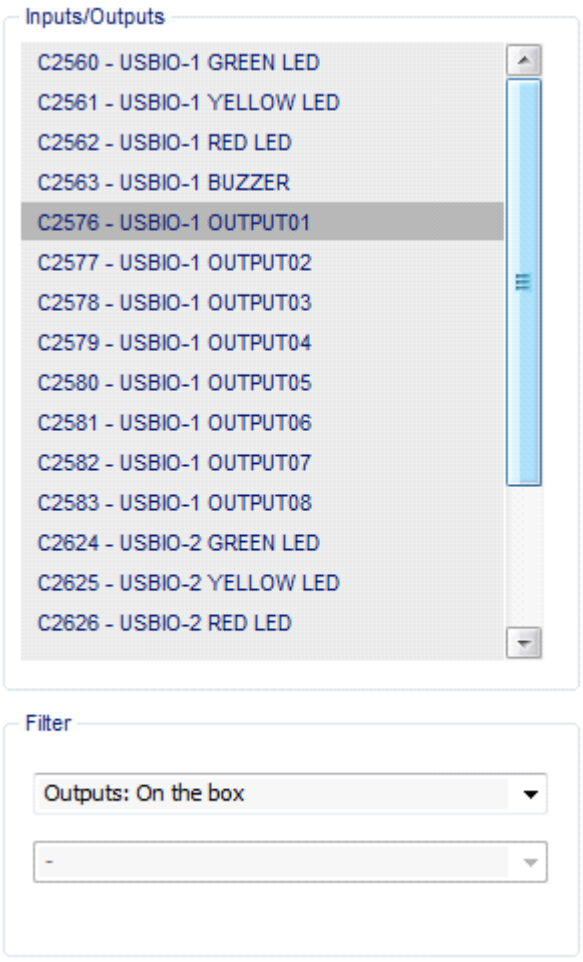
If the event has a “silent alarm” profile, no mail will be sent to any of the recipients!

9 Activate outputs

To activate an output, open the Input/Output Behaviour window via **System > Behaviour > Input/Output Behaviour**.

Select an output from one of these groups:

- ***On the box***: outputs on the OTB IO cards, 8 outputs on the first set (MIO and EIO cards) and 8 outputs on the second set.
- ***Network***: outputs available on the Net IO modules, connected to the Ethernet.
- ***VM22A***: an output that activates the corresponding loudspeaker on the VM22A audio.
- ***Workbits***: virtual outputs that can be used to store internal states.



Use the filter option to reduce the list.

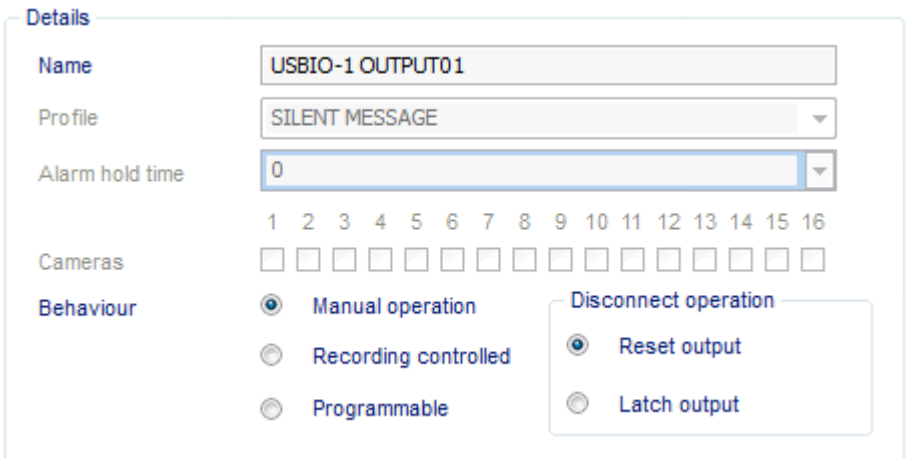
Click ‘Save’ to apply the new settings.

Warning:

Outputs that are already used for another operation cannot be modified here!

9.1 Manual operation

Select the desired output and choose “Manual operation”.



The output will thus need to be switched by a user from the client software.
For more information on activating an output manually, read the FastTrace 2 Users’ Manual.

You also have to define what action needs to be taken when closing the client software application:
- Reset output: the output always resets to idle state when closing the client application;
- Latch output: the output remains in the selected state, even after closing the client application.

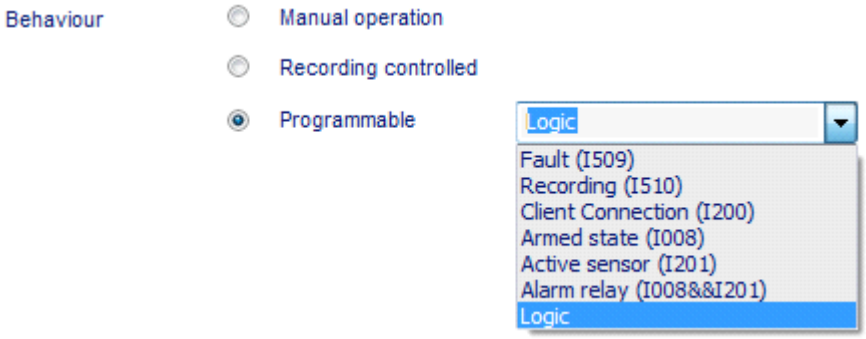
9.2 Recording controlled

This output will be used by video cameras when recording.

For controlling an output while recording, read the FastTrace 2 User’s manual.

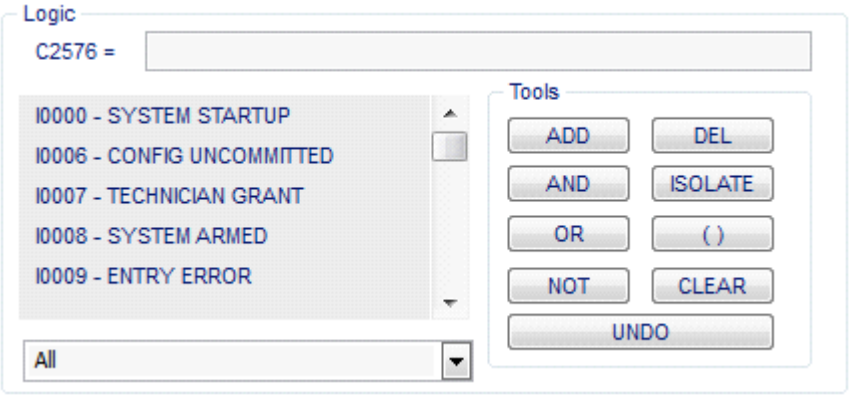
9.3 Programmable output

This option activates an output in function of a condition or event. The condition is specified in the drop-down list:



With the last option – “Logic” – you can specify a specific condition, selecting particular inputs linked with AND and OR functions. Brackets allow to modify the order of evaluation (which is normally from left to right). The state of an input can be inverted (NOT function) and the isolate state of an alarm can be selected (ISOLATE). Select an input from the list and click ‘ADD’ (in the “Tools” section) to insert it at the current position. On error, click ‘DEL’. To clear the whole line, click ‘CLEAR’.

Click the ‘NOT’ button before adding an input if you want to invert its state.
Click the ‘ISOLATE’ button just after adding an input if you want to read its operational state (isolated or not). The letter M appears in front of the number of the selected input.

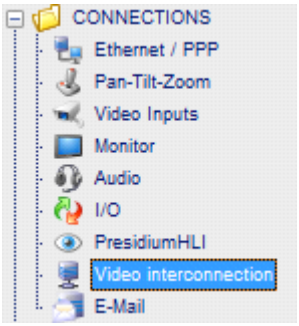


Example: I2144 AND I2145 OR M2146 AND NOT I2145.

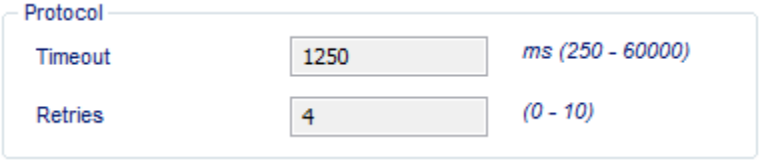
10 Video Interconnection

The interconnection as described underneath deals with interconnection of the FastTrace 2 with the Xtralis S3100 system.

Open the Video Interconnection window via **System > Connections > Video interconnection**.

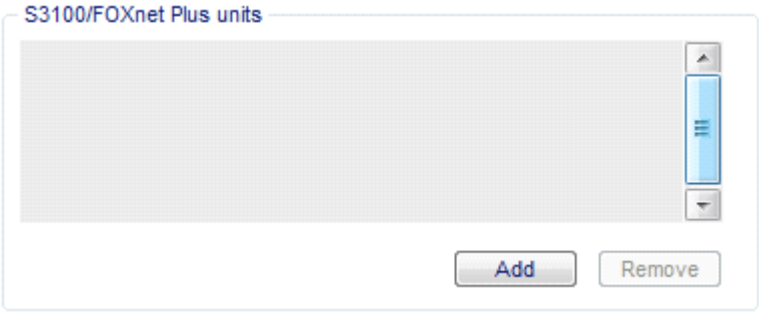


Enter the desired protocols. The default values normally suffice, but can be increased on slower networks if you observe communication faults between the interconnected devices.

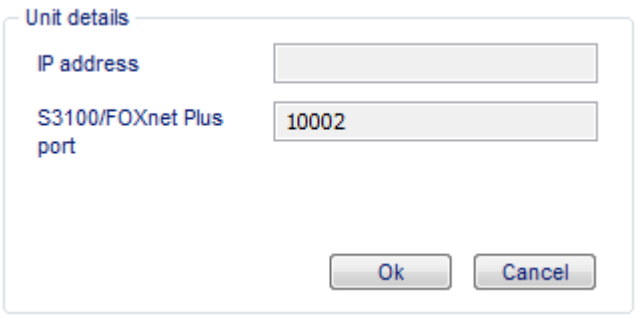


You can add multiple S3100 security panels to the list of devices the FastTrace 2 video system should interconnect with.

Click ‘Add’.



To the right this section will appear:

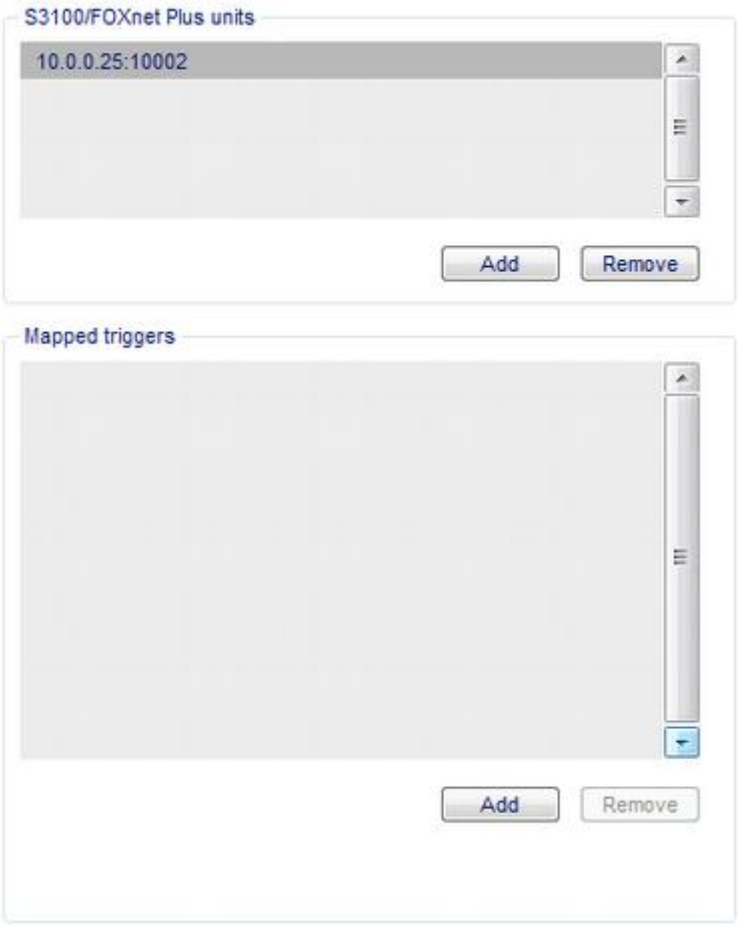


Enter the IP address of the S3100 security panel. If necessary also modify the port for communication (as defined in the security panel).

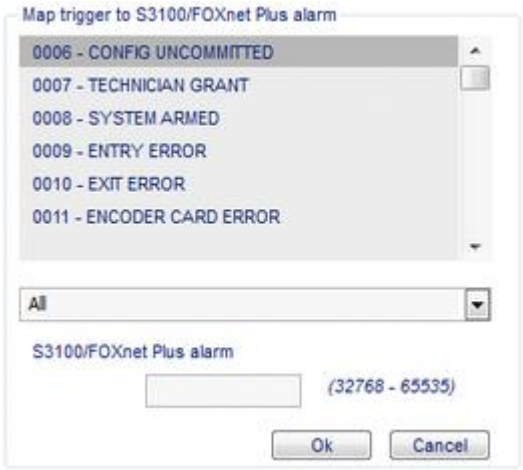
Each S3100 security panel can activate one of the 8 available virtual inputs on the FastTrace 2 video system.

See also FCU Configurator. Please read Alarm profiles for more information on configuring the virtual inputs.

Next, select the S3100 security panel from the list and click ‘Add’ in the “Mapped triggers” section.



To the right a new section will appear:



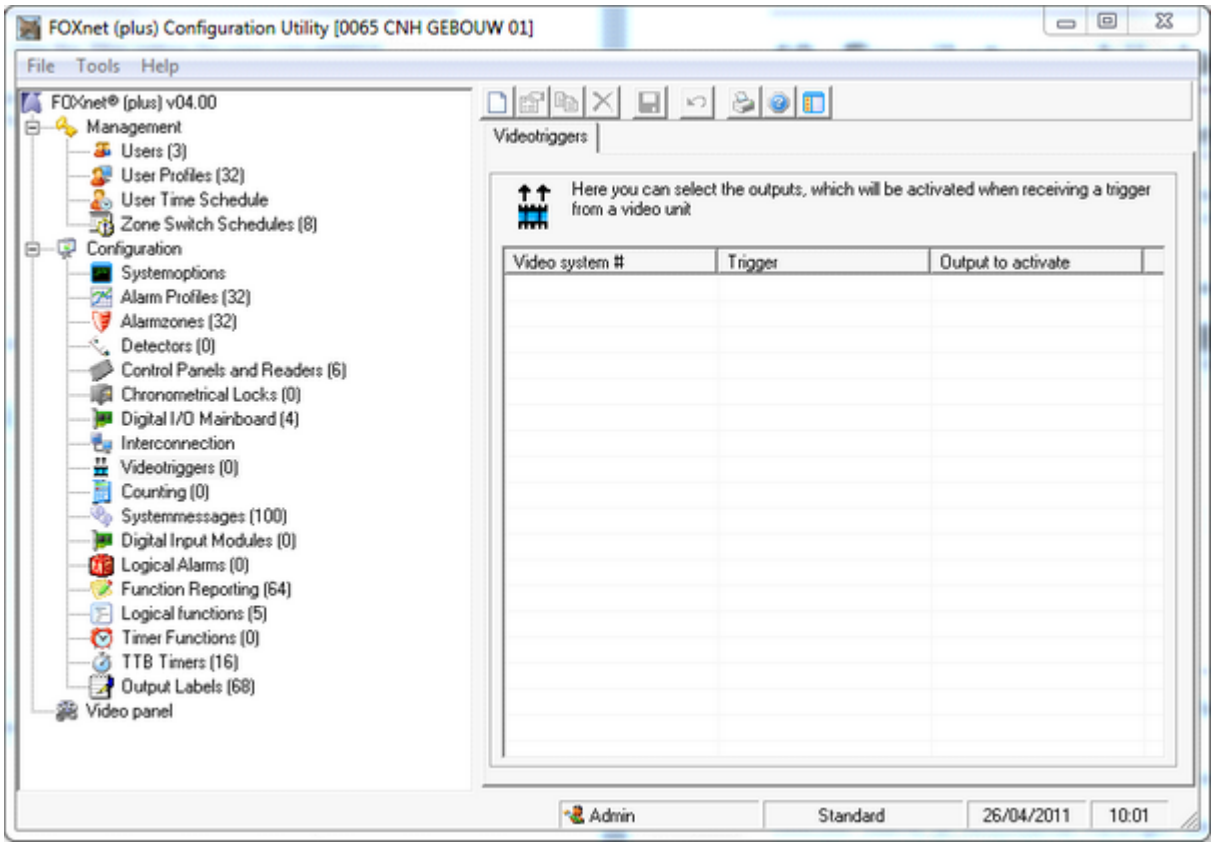
Select an alarm and associate the alarm to a trigger. Use the filter option for your convenience.

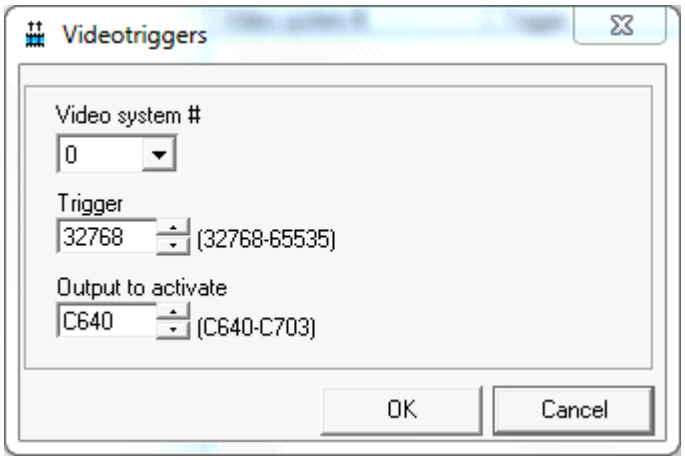
In the S3100 security panel the trigger needs to be associated to an output. This output will be activated when detecting the associated event (e.g. hard disk error).

Click ‘Save’ to apply the new settings.

Hint:

In the S3100 Configurator, open Video triggers and click ‘New’ to associate the selected trigger to the output.





Interconnection also works with the older FOXNet(Plus) security panels.

11 PIR settings

11.1 Required PIR firmware

For a correct functioning of the PIR alarm processing, a minimal PIR firmware version 2.00 is required. Previous firmware versions also work with RS485 communication, but do not support all features (e.g. Alarm Management).

11.2 Connecting the PIRs

The PIR should be connected to the FastTrace 2 server. You have three options:

1) using an RS485 cable and connecting the cable from the PIR to the main I/O card of the FastTrace 2 server;
2) using the USB to RS485 8 channel distribution unit;
3) using a USB to serial port RS485 convertor and connecting the PIR to the convertor by means of an RS485 cable.

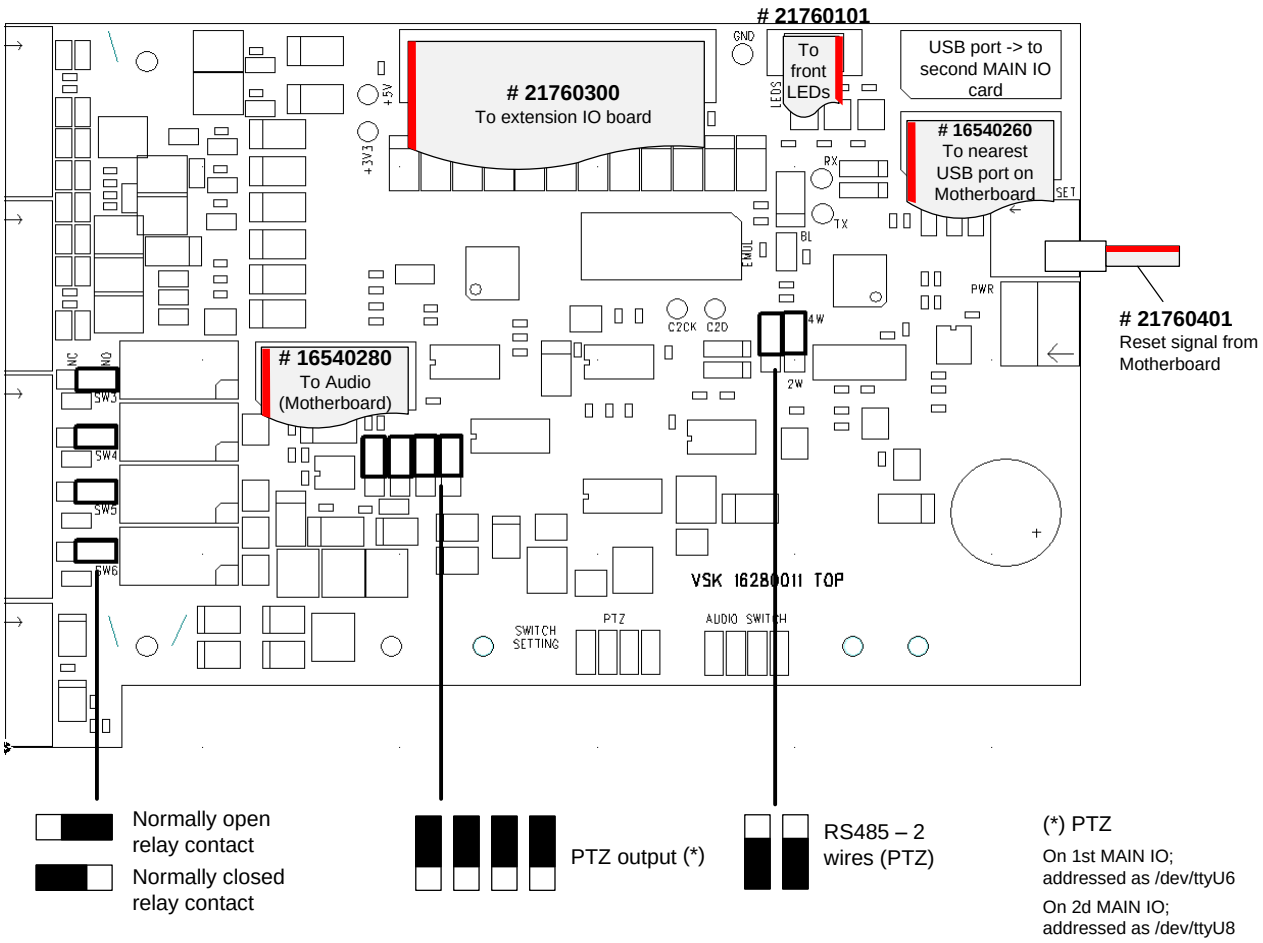
Mind:

From firmware version 2.6 onwards, a separate PIR-HLI application license is required to configure the PIR devices. Please consult Application license for more information!

11.2.1 Connecting the PIR detector directly to the FastTrace 2 server (Main I/O card)

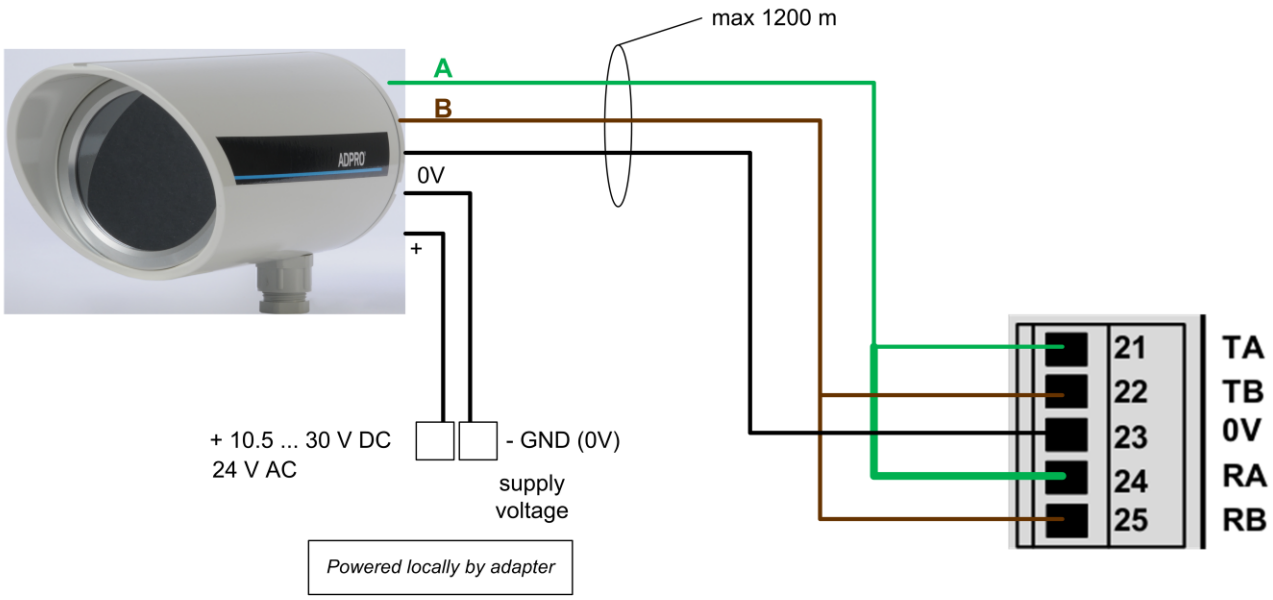
Connect the PIR device(s) (multiple PIRs need to be set up in cascade) to the FastTrace 2 by connecting the RS485 cable of the PIR closest to the FastTrace 2 to the main I/O card of the FastTrace 2 server.
The PIR(s) must be connected to the appropriate terminals on the FastTrace 2 Main I/O card.

Set the dipswitches on the Main I/O to PTZ output and RS485 – 2 wires. (*see* *Serial PTZ on MIO card*)



Also bridge the following connections:

- TA (pin 21) with RA (pin 24)
- TB (pin 22) with RB (pin 25)



Locally powered PIR detectors can be placed at the maximum distance of 1200 m for 485 cables, but do mind that this remains a 3 lines communication (RS485 + 0V).
It is also important not to have a difference in earth potential between FastTrace 2 and PIR.

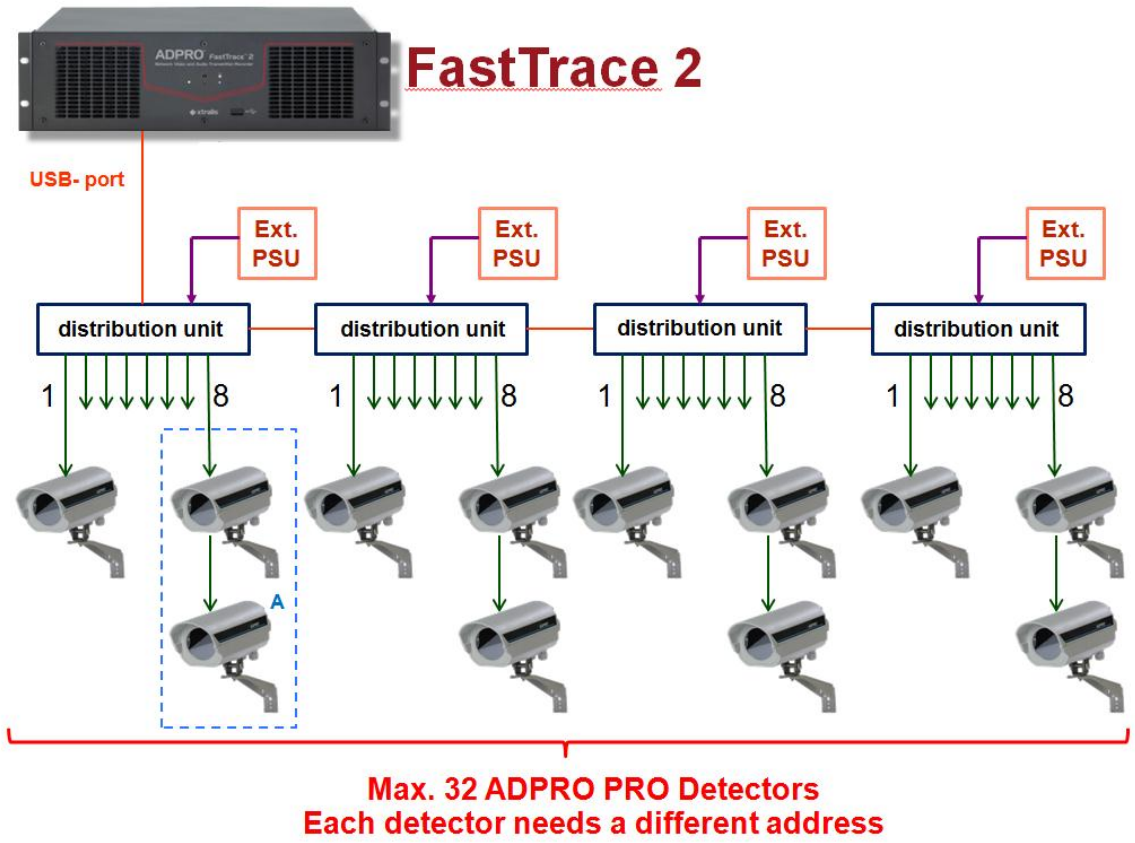
11.2.2 Connecting the PIR detector to the FastTrace 2 server using the USB to RS485 8 channel distribution unit

*Please read the technical data sheet **19532060** on the **USB to RS485 8 channel distribution unit** for further detailed information!*

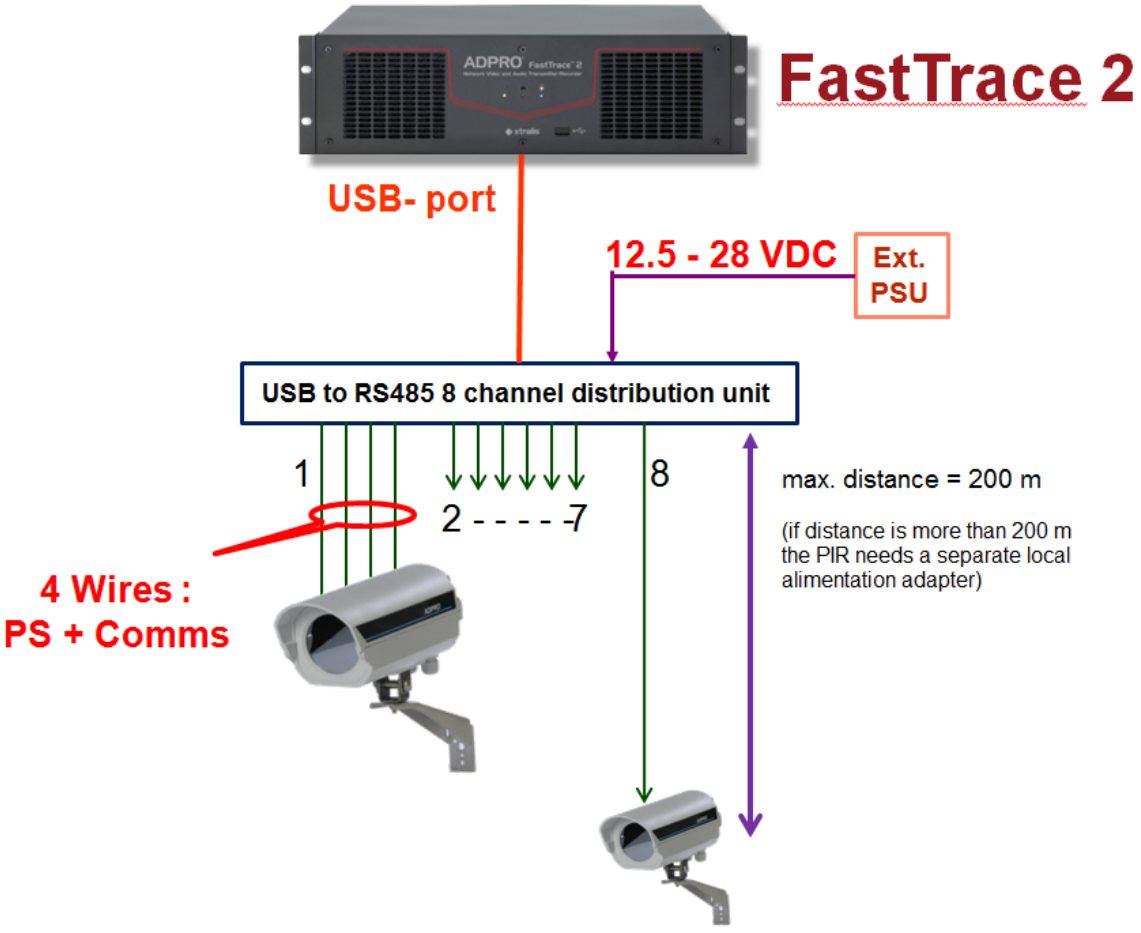
The USB to RS485 distribution unit provides 8 channels (1 PIR unit per channel) to easily connect and configure the PIR units to the FastTrace 2 server.

Up to 8 PIRs can be connected through star wiring to the USB to RS485 distribution unit. Only the 485 bidirectional communication of the PIRs is used, we do not use the mechanical PIR tampers. It is possible to connect 4 distribution units *in cascade* (= only one of the 4 distribution units need to be connected to the FastTrace 2, but the cables between the other units should not exceed more than 1 metre), so a maximum of 32 PIR devices can be supported by the FastTrace 2.

The unit contains a USB connection port for communication with the FastTrace 2 video system. Mind: only the TTY2 can be used! The USB cable between distribution unit and FastTrace 2 server should as short as possible (and certainly not more than 1 metre).

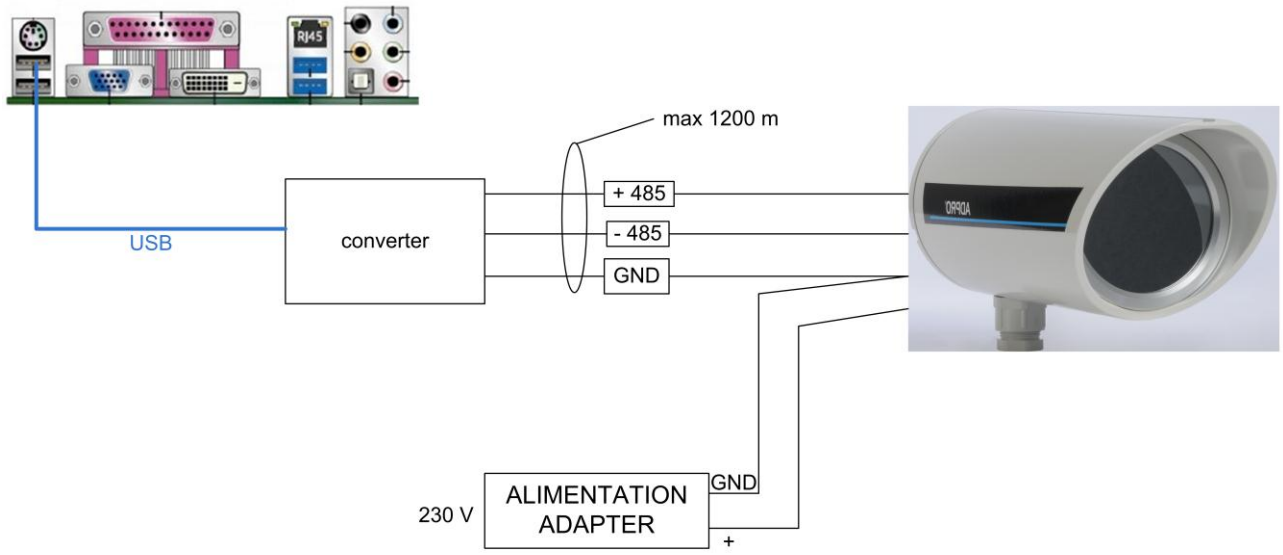


A detailed view of one connected distribution unit:


FastTrace 2
USB- port
12.5 - 28 VDC
Ext. PSU
USB to RS485 8 channel distribution unit
1
2 - - - - 7
8
4 Wires :
PS + Comms
max. distance = 200 m
(if distance is more than 200 m the PIR needs a separate local alimentation adapter)

11.2.3 Connecting the PIR detector to the FastTrace 2 server using a USB to serial port RS485 converter

Connect the PIR detector to the converter and plug the USB cable of the converter in the ttyU2 USB port of the FastTrace 2 server.



Locally powered PIR detectors can be placed at the maximum distance of 1200 m for 485 cables, but do mind that this remains a 3 lines communication (RS485 + 0V).
It is also important not to have a difference in earth potential between FastTrace 2 and PIR.

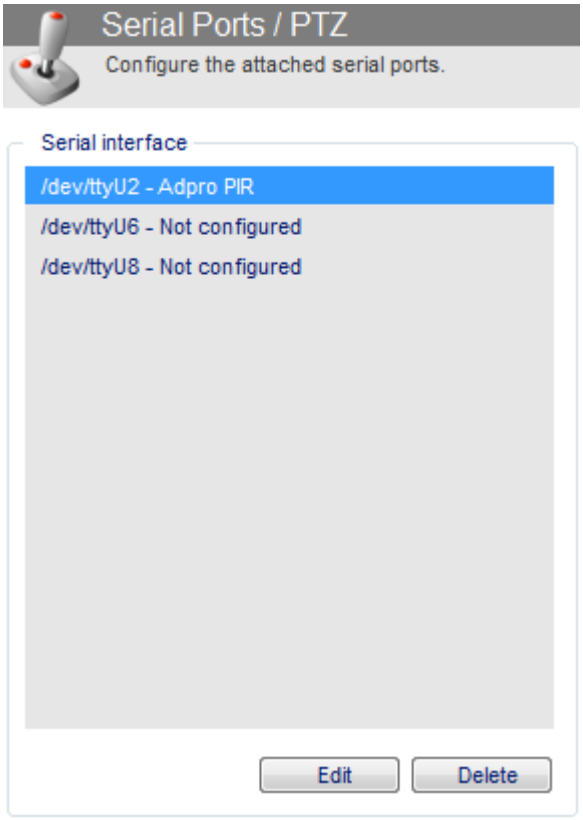
The above drawing shows you the Intel DH61BE motherboard. Please check Required motherboard for the specific location of the ttyU2 USB port on the specific motherboard of your video system.

The USB to serial port RS485 converter needs to be ordered separately!

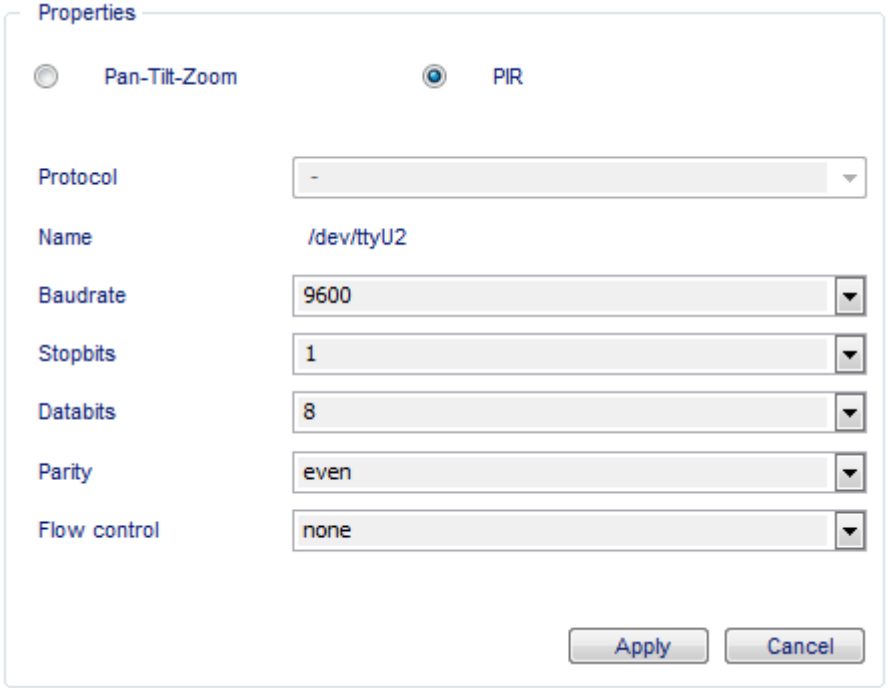
11.3 Configuring the software setting

11.3.1 Configuring the serial port

You need to set the serial port to PIR. Open the *Serial Ports / PTZ* window via **System > Connections > Serial Ports / PTZ**.



Select the desired serial interface from the list and click **Edit**. The *Properties* section will appear to the right.



Choose the *PIR* option. By default all parameters are attributed. There's no need to change any of the settings.

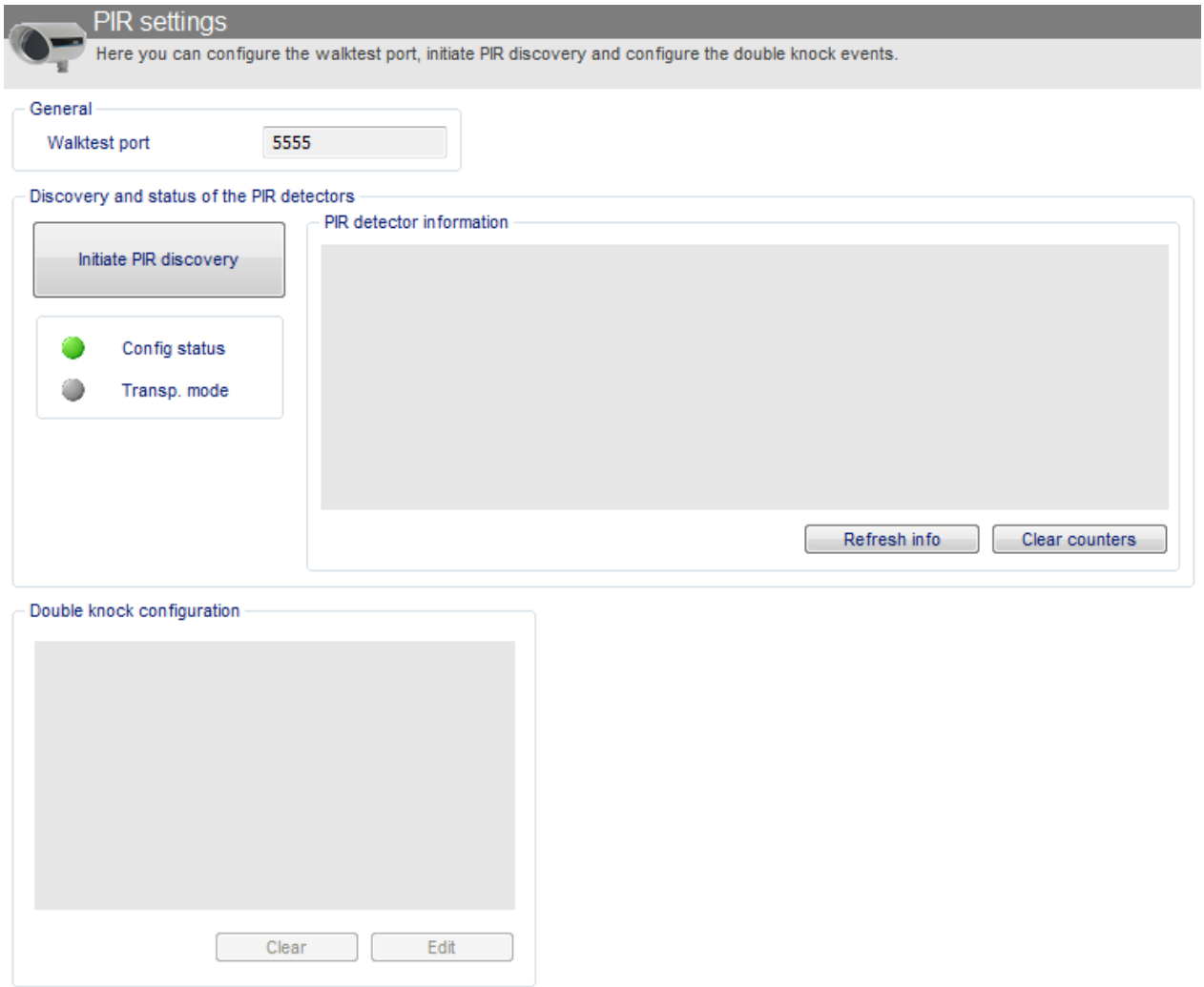
Mind:

When using the USB to RS485 distribution unit or the USB to serial port RS485 convertor, your only option is to use the /dev/ttyU2 USB port.

When connecting your PIR directly to the Main I/O of the FastTrace 2 server (using an R485 cable), you will have to use either the /dev/ttyU6 USB port (for the first Main I/O card) or the /dev/ttyU8 USB port (for the second Main I/O card). These ports are automatically detected by the FastTrace 2 client software.
(see Connecting the PIR detector directly to the FastTrace 2 server (Main I/O card))

11.3.2 Initiate the PIR discovery

Open the *PIR settings* window via **System > Behaviour > PIR settings**.



11.3.2.1 General

In this section you can set the *walk test port*. This port will be used for iPhone integration in a future version of the FastTrace 2 Client software.

The default *walk test port* is set to 5555.

11.3.2.2 Discovery and status of the PIR detectors

By default the status is set to configuration status (shown by the green ball). The transparent mode will be used for iPhone integration in a future version of the FastTrace 2 Client software.

Click the button **Initiate PIR discovery** to search the FastTrace 2 servers for any connected PIR devices.

The list is shown in the section *PIR detection information*:

PIR detector information (Last requested at 2012/03/30 - 15:43:44)
|PIR|Name |Discovered|Presence|Time outs|Pkt Errors
1 | |No |No | 0| 0
2 | |No |No | 0| 0
3 | |No |No | 0| 0
4 | |No |No | 0| 0
5 | |No |No | 0| 0
6 | |No |No | 0| 0
7 | |No |No | 0| 0
Refresh info
Clear counters

Click the **Refresh info** button to execute the search for connected PIR devices anew.

Click the **Clear counters** button to delete the numbers in the *Time outs* and *Pkt Errors* lists.

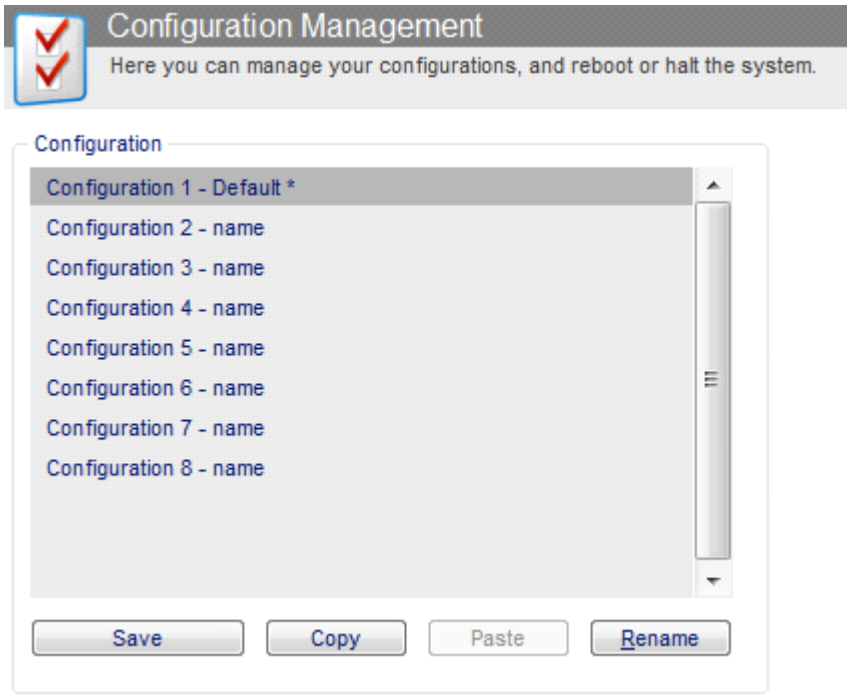
11.3.2.3 Double knock configuration

The double knock configuration is used to activate the alarm only when you have configured one or multiple events that have to occur.

12 Configuration

12.1 Storing a configuration

Open the “Configuration Management” window via **System > Maintenance > Configuration Management**.



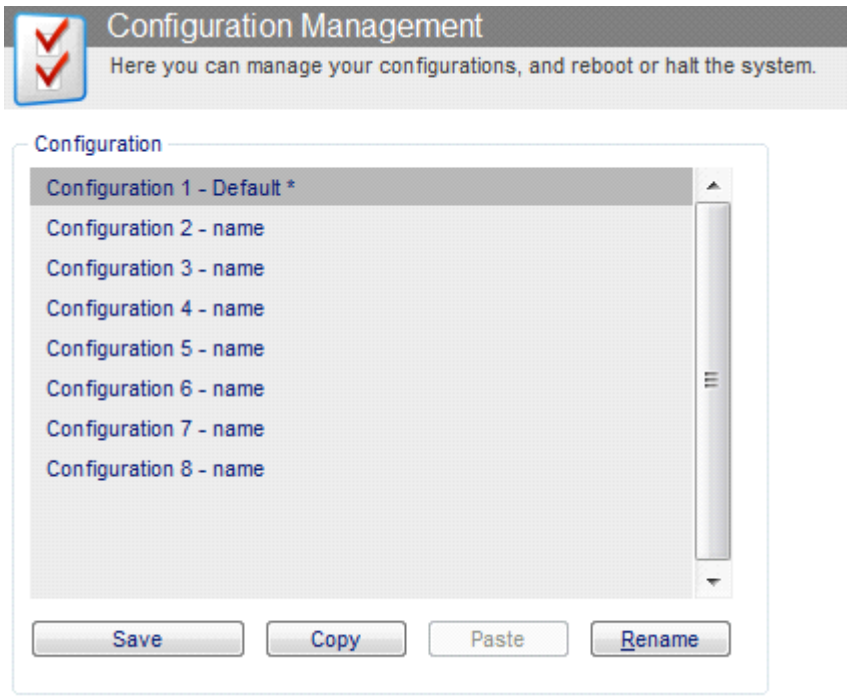
The video system can store up to 8 different configurations. Only 1 configuration can be active. The active configuration is marked with an asterisk.

Select a configuration. Click **Save** to store the current settings under the selected configuration. Click **Rename** to provide a new description to the selected configuration. It is recommended to use a meaningful and relevant description.

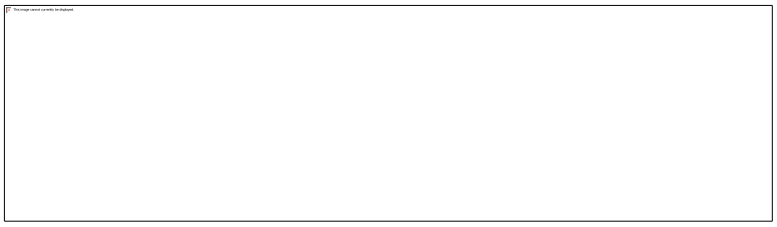
You can also copy the selected configuration by clicking **Copy**. At that moment the **Paste** button becomes active. You can now choose another configuration and click **Paste** to provide the same settings to the newly selected configuration. Afterwards (small) modifications can be made to the new configuration.

12.2 Activating a configuration

Open the *Configuration Management* window via **System > Maintenance > Configuration Management**.



Select a configuration from the list and click **Activate configuration** in the *Boot* section.



When you click ‘Factory defaults’ all modified configurations will be deleted. Your FastTrace 2 video system will also be given the default IP address 10.0.0.10!

You can restart the FastTrace 2 video system by clicking **System restart**. If you want to stop the video system, click **System halt**. It is recommended to halt the system before switching off power.

13 Configuring analytics

It is very important to keep in mind that for the video perimeter detection and the video loitering detection a separate application license is required.

With the FastTrace 2 there is a maximum of 4 analytic channels on the types of analytics mentioned above. This means that you have to carefully choose the number of analytics you want to use on a specific site. You can, for instance, have 3 perimeter detection channels and 1 loitering channel. The total amount of analytic channels cannot be higher than 4, so in this example you have reached your maximum amount of analytic channels!

The FastTrace 2☒ can handle up to 16 analytics streams!

Mind

When you open the analytics configuration pages in the FastTrace 2 client software, the Client takes CMS priority. It is thus impossible to have any conflicts with the monitoring and alarm management software.

13.1 FastTrace™ 2 IntrusionTrace

IntrusionTrace stands for full outdoor perimeter detection analytics.

13.1.1 About the FastTrace 2 Perimeter Detection analytic

The FastTrace 2 perimeter detection analytic **IntrusionTrace**:

- is able to detect human intrusions in a *sterile* zone. A *sterile* zone is (part of) a scene where human intrusions are not allowed. It is usually a zone that is nearly free of obstacles such as trees or cars.
- has a very low probability of false alarms from small animals, clouds, wind, rain or snow.
- does not depend on the resolution or frame rate of the camera.
- requires a minimum detection area of 6 m (19 ft) width and a maximum horizontal FOV of 25 m (82 ft) for reliable detection.
- is based on 3D measures and therefore requires a 3D calibration using a person once in a front position and once in a rear position.
- could mask parts of the image to avoid false alarms due to flashing light, trees, cars, on screen display of time … et cetera.
- uses *Ground Region of Interest*: any object whose lowest point (= ground position) is outside of the GROI will not trigger any perimeter detection. It is advised to use a larger GROI zone than the real ground zone surveyed. It is also advised to include the lower edge of the image to make sure that persons at the bottom of the image are not excluded from detection.

A *detection zone* is a zone on the ground where intruders trigger an alarm. A *trigger line* is a line on the ground, which intruders should not cross. The alarm is only issued if the person(s) remain(s) at least 2 seconds and move(s) for at least 0.8 metres (3 ft).

When both trigger lines and detection zones are defined, an alarm will be issued if one of the trigger lines **or** one of the detection zones detects an intrusion.

13.1.2 Scope

The FastTrace 2 Perimeter Detection analytic is an image analysis tool able to detect human intrusion in a sterile zone, i.e. a (part of a) scene where human intrusions are not allowed. Good examples of sterile zones are the surroundings of a prison, the surroundings of a nuclear plant, a military or civilian strategic site … etc. The sterile zone should be (nearly) free of obstacles such as cars, trees … etc.

The Perimeter Detection analytic uses advanced algorithms to maximize target detection and tracking under a wide range of environmental conditions. It therefore has a very low probability of false alarms from animals, clouds, wind, rain or snow.

13.1.2.1 Suitable scenes

The following scenes can be configured for perimeter detection:

13.1.2.2 Unsuitable scenes

13.1.3 Camera

13.1.3.1 Resolution and frame rate

Whatever the resolution of the camera, the system is providing the analytics with CIF images at a frame rate of 5 frames per second. The resolution and frame rate used for monitoring or continuous/event recording have no influence at all on the Perimeter Detection analytic.

Mind:

Arecont cameras do not support the analytics stream and can therefore not be used for Perimeter Detection!

13.1.3.2 Field of view (FOV)

The minimum detection area requirement is 6 m (19 ft.) width, i.e. if there is only a 2 m (6 ft.) gap between a building and a fence, it will not be reliable.

The maximum horizontal FOV is 25 m (82 ft.), to avoid missed detection of too small targets.

13.1.3.3 Position

It is advised to avoid large parts of the FOV not used for detection. Large areas of the sky or large areas not monitored render the perimeter detection unreliable.

The Perimeter Detection uses perspective compensation; hence it is important that the FOV is not too obtuse. A target in the background on the left edge of the FOV must be more or less the same size as the same target in the background on the right edge of the FOV. If that same target moves to the front of the FOV, it should be getting bigger.

For optimal results, it is advised that the target closest to the camera has its feet at the base of the camera FOV, and its head at the furthest detection distance is just below the top of the FOV of the camera. Ensure the FOV is clear, with minimum views of foliage and obstructions that provide cover for intruders.

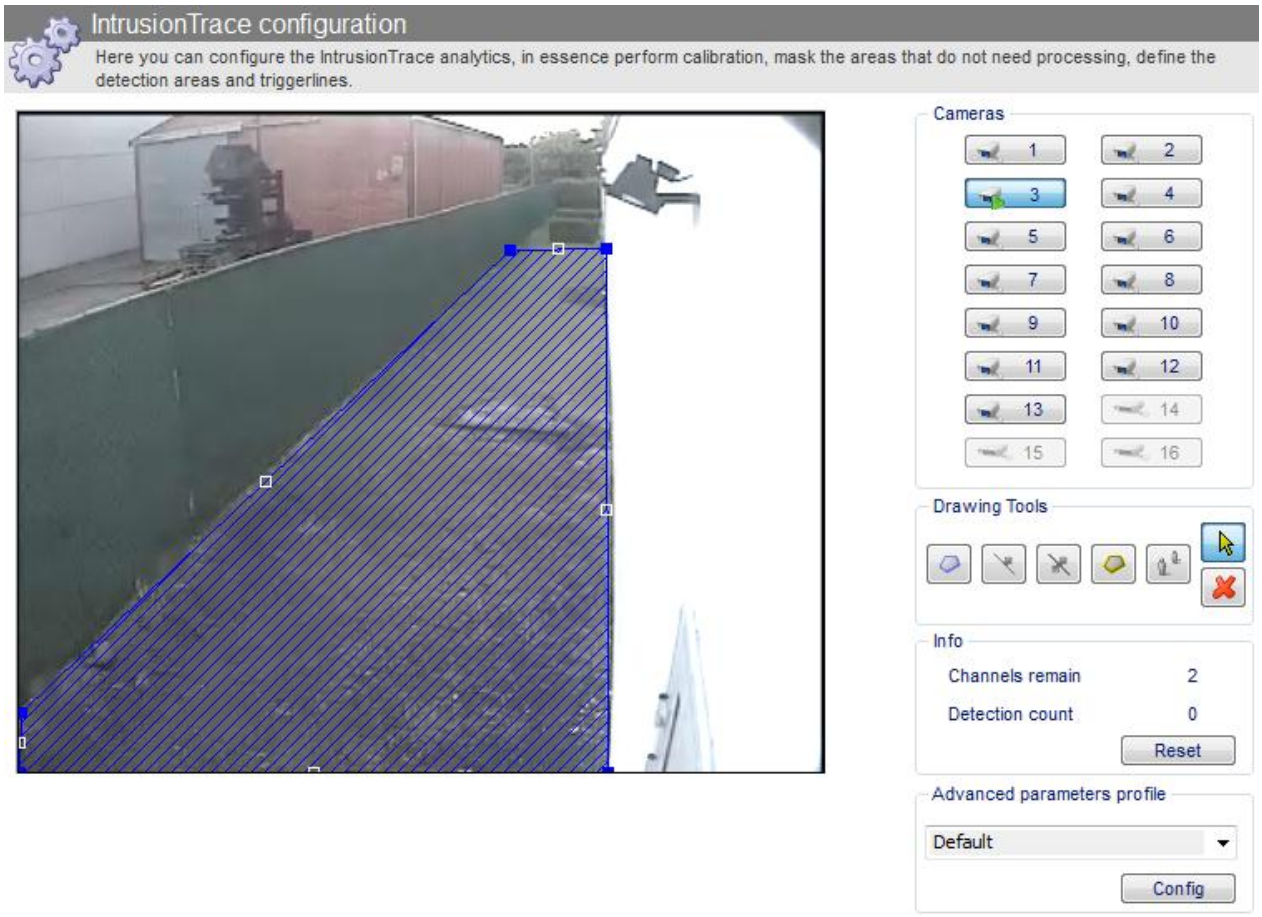
The perspective characteristics used in Perimeter Detection will not function as expected when the camera is mounted too high. The camera should at least be at a height that is out of reach of intruders. This should be between 3 to 6 metres (9.8 to 19.7 ft). The ideal height is 4.2 m (14 ft), as this allows the detection algorithms to function and is high enough to prevent tampering with the camera.

The *dead zone* of a camera – the area under the camera that the camera cannot view – should be covered by another camera's FOV. The area just in front of the dead zone can also be vulnerable to fast moving targets. It is a good practice to ensure that the FOV of the camera covering the dead zone includes the dead zone plus an extra 10 to 15% of the area adjacent to the dead zone.

13.1.4 Configuration

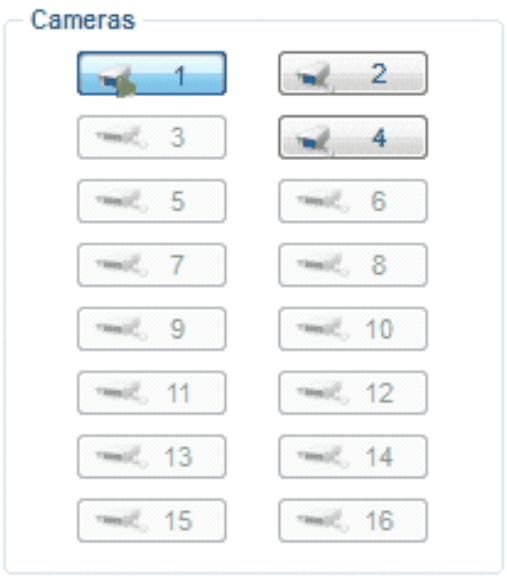
13.1.4.1 Perimeter configuration interface

In the FastTrace 2 Client, open **System > Behaviour > Analytics > IntrusionTrace**.



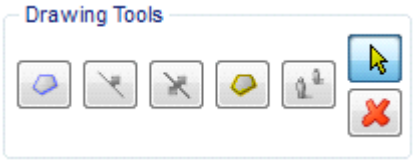
13.1.4.2 Cameras section

Select the desired camera you want to configure perimeter detection for. Only one camera at the same time can be selected.



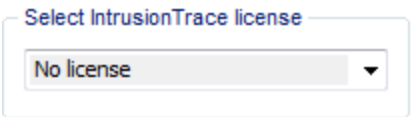
13.1.4.3 Drawing Tools section

You can add several perimeter detections settings to the image. Use the drawing tools to add these settings. All necessary information about the tools is shown under the image when you click the button.



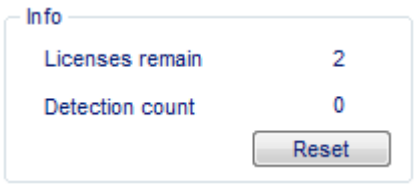
Icon	Description
	Draw the detection ground zone. Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be hatched with blue lines, thus creating a blue zone. You can also click the right mouse button to close the drawing. Detection areas define the regions where objects are detected as valid. They must pass the detection criteria while in these areas in order for an alarm to occur. A maximum of 16 polygon areas can be drawn. These areas can overlap. See also Detection zones.
	Draw one or multiple unidirectional trigger lines. Trigger lines are used to trigger an alarm when an object moves in a certain direction (= i.e. the direction of the arrow). Click the right mouse button to stop drawing trigger lines. A maximum of 16 trigger lines can be drawn. See also Trigger lines.
	Draw one or multiple bidirectional trigger lines. Trigger lines are used to trigger an alarm when an object moves in a certain direction (= i.e. the direction of the arrows). Click the right mouse button to stop drawing trigger lines. A maximum of 16 trigger lines can be drawn. See also Trigger lines.
	Draw a mask area. Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be hatched with yellow lines, thus creating a yellow mask zone. You can also click the right mouse button to close the drawing. Mask areas define the regions that will not be processed by the analytics module. A maximum of 5 polygon areas can be drawn. These areas can overlap. See also Mask zones.
	See Calibration.
	Select objects by clicking them.
	Delete the selected object.

13.1.4.4 Select IntrusionTrace license section



Choose the desired IntrusionTrace license. If there is no license available, you will either need to order a new license (credits can be ordered through the license portal; see Application License Guide) or transfer one of your IntrusionTrace licenses.

13.1.4.5 Info section

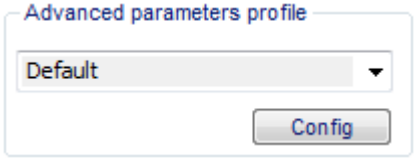


In the “Info” section you can see how many “licenses remain”. This indicates the number of remaining perimeter detection licenses (i.e. the subtraction between the total number of licenses and the number of used licenses). You need to delete **all** trigger lines and **all** detection zones from a camera and click ‘Save’ to make sure the remaining channels number is increased again.

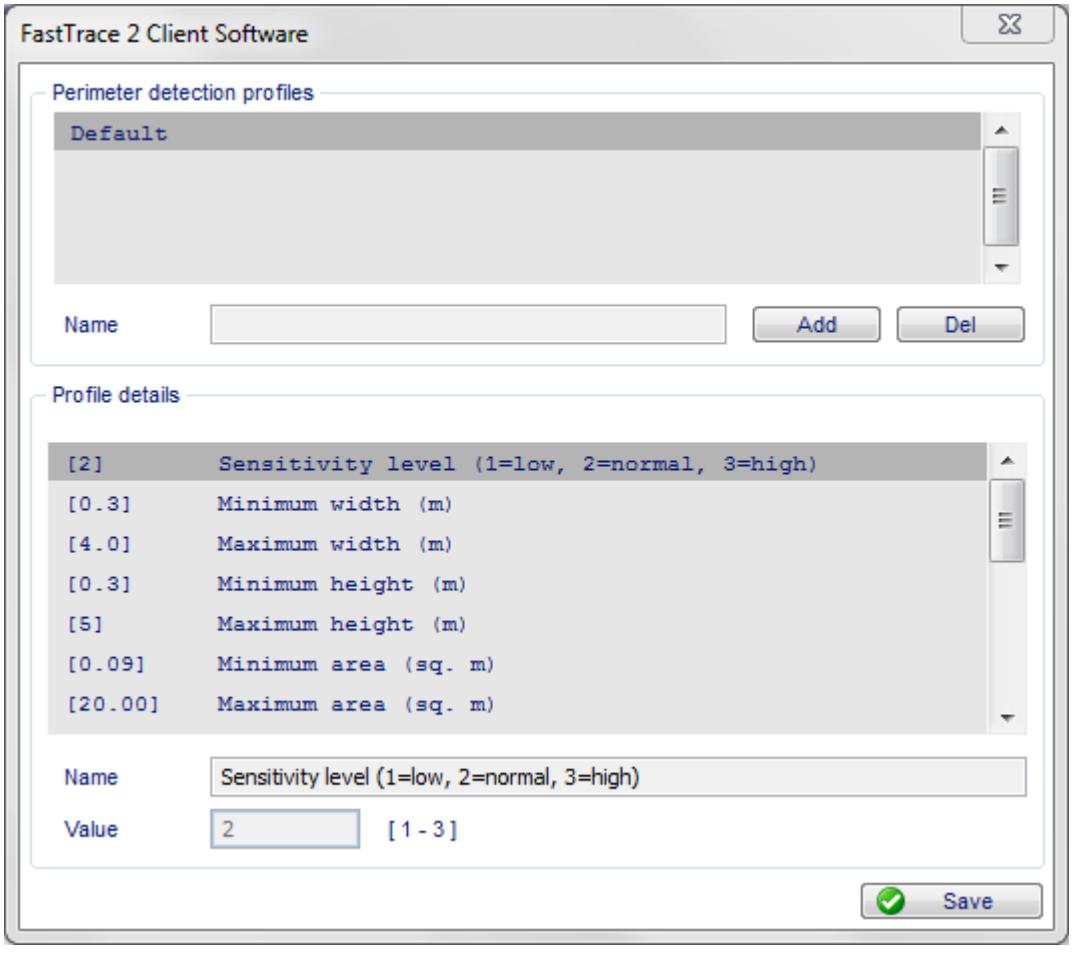
The “Detection count” indicates the number of detections while the configuration was running. You can reset the detection count by clicking ‘Reset’.

13.1.4.6 Advanced parameters profile section

You can choose a specific perimeter detection profile from the section *Advanced parameters profile*.



By default there is a default profile that has been attributed to the perimeter detection. You can change this profile or add new profiles. Click **Config**.

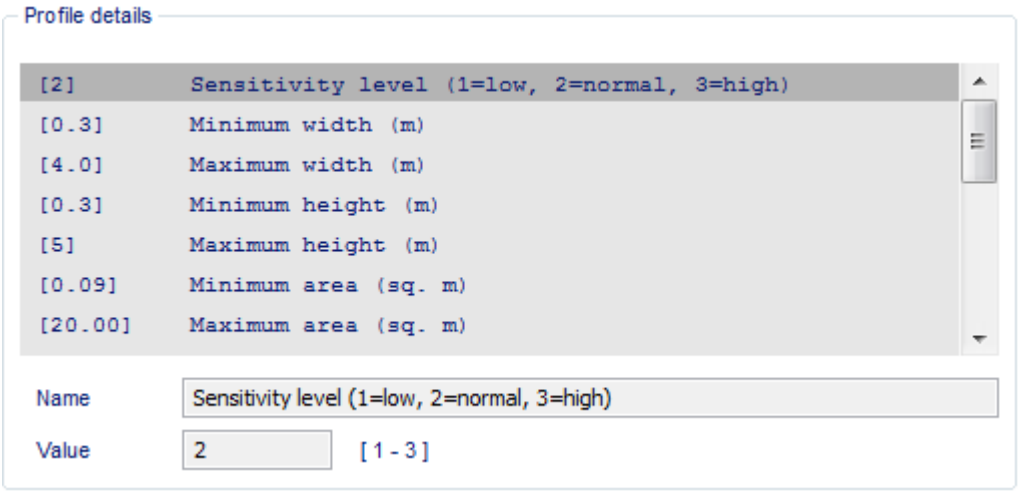


13.1.4.6.1 Profile details

A perimeter detection profile has got the following parameters. These parameters can be easily changed by adapting the value at the bottom of the section *Profile details*.

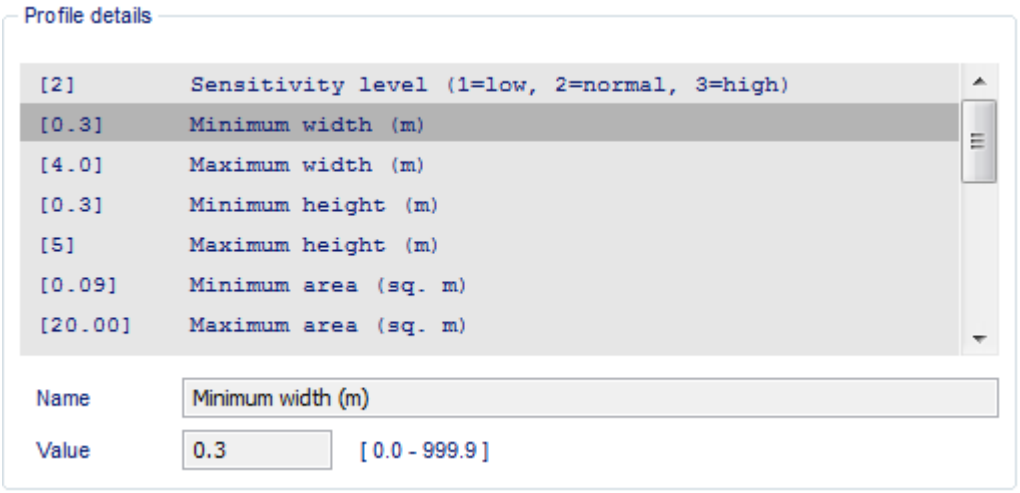
Sensitivity level

You can change the level of contrast sensitivity to either low (value = 1), normal (value = 2) or high (value = 3). When set to high, the system will detect lower contrasted objects, while setting the sensitivity level to low will limit the amount of false alarms.



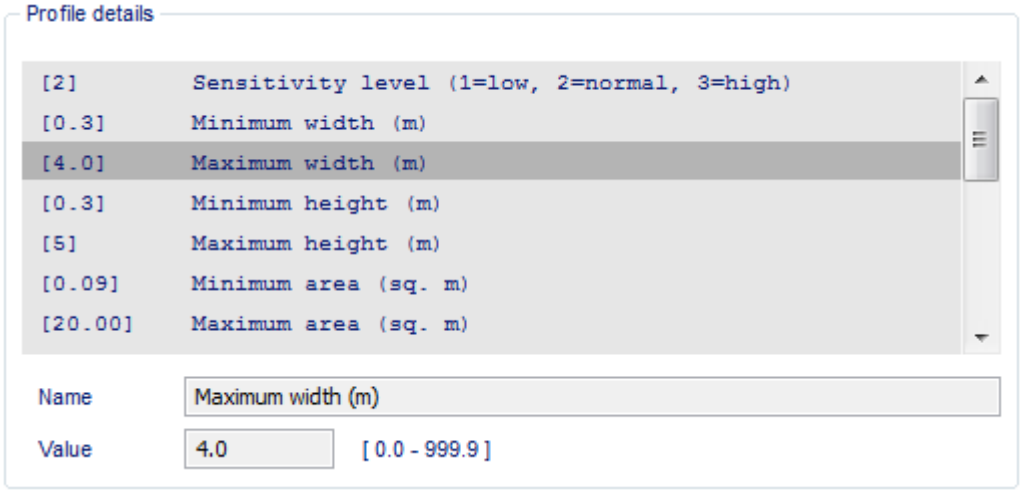
Minimum width (m)

Setting the minimum width is essential to avoid detection of thin objects. An object will not generate an alarm if its width is less than the specified value. The value is expressed in metres. For detecting humans a typical minimum width is 0.3 metres.



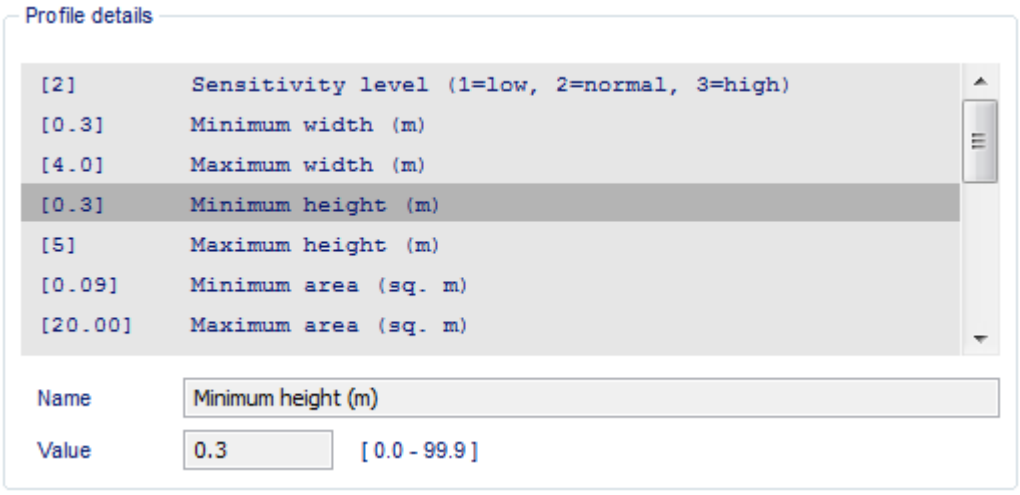
Maximum width (m)

Setting the maximum width is essential to avoid detection of large objects. An object will not generate an alarm if its width is greater than the specified value. The value is expressed in metres. A group of persons may appear as a single large object, so a maximum width of 4 metres is typical to detect humans.



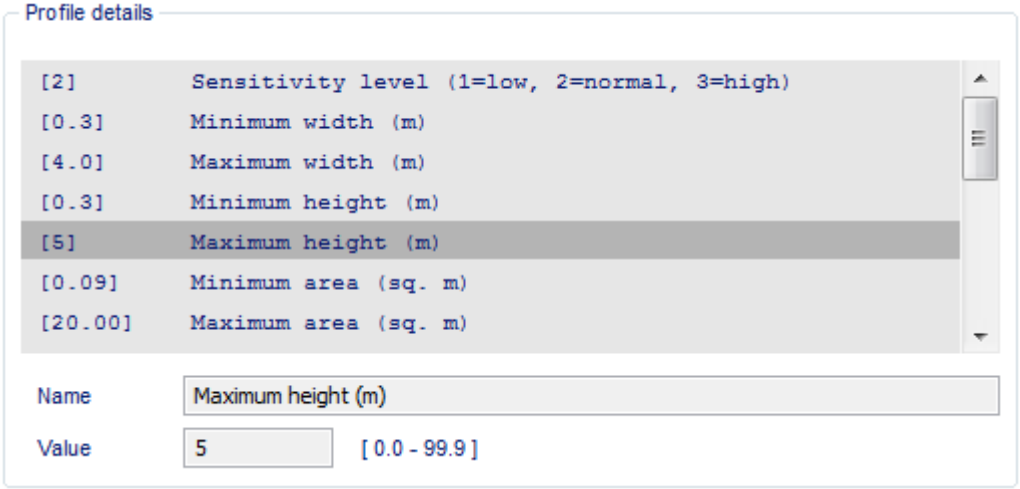
Minimum height (m)

Setting the minimum height is essential to avoid detection of small objects. An object will not generate an alarm if its height is less than the specified value. The value is expressed in metres. For detecting humans a typical minimum height is 0.3 metres, because he/she could be crawling.



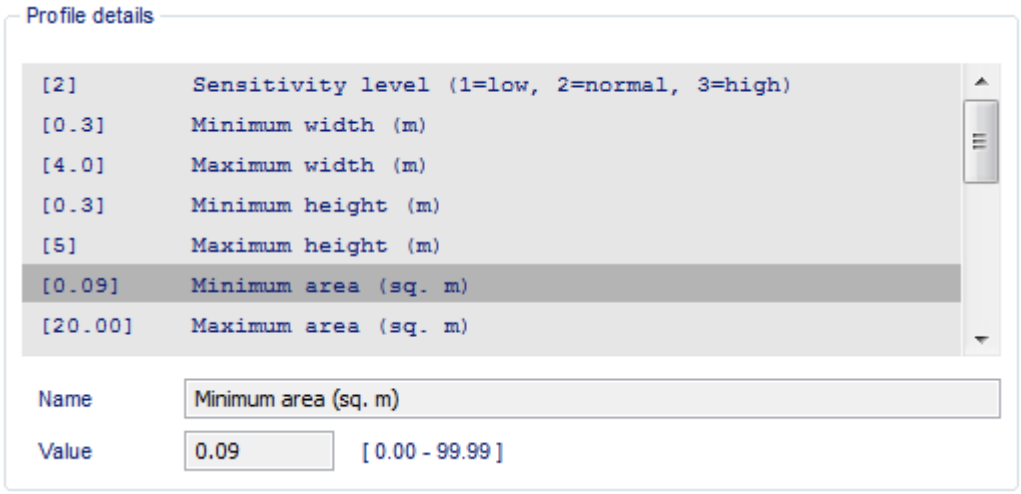
Maximum height (m)

Setting the maximum height is essential to avoid detection of tall objects. An object will not generate an alarm if its height is higher than the specified value. The value is expressed in metres. For detecting humans a typical minimum height is 5 metres, because a single person carrying a large object (e.g. a ladder) can appear as a very tall object.



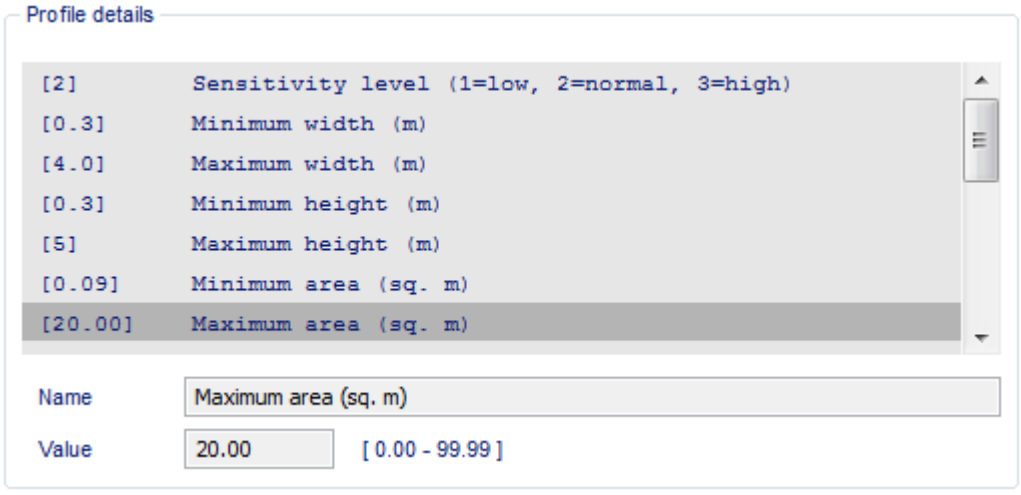
Minimum area (sq. m)

Setting the minimum area is essential to avoid detection of small objects. An object will not generate an alarm if its surface is less than the specified value. The value is expressed in square metres. For detecting humans a typical minimum area is 0.09 square metres, because a rolling human may have a really small surface (0.3 m width x 0.3 m height).



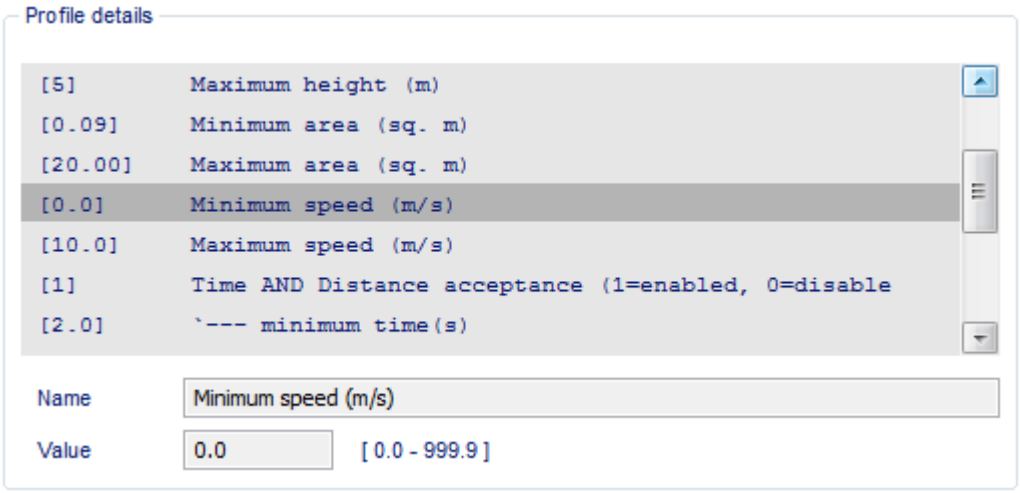
Maximum area (sq. m)

Setting the maximum area is essential to avoid detection of large objects. An object will not generate an alarm if its surface is greater than the specified value. The value is expressed in square metres. For detecting humans a typical minimum area is 20 square metres, because a group of persons may appear as a single large object (4 m width x 5 m height).



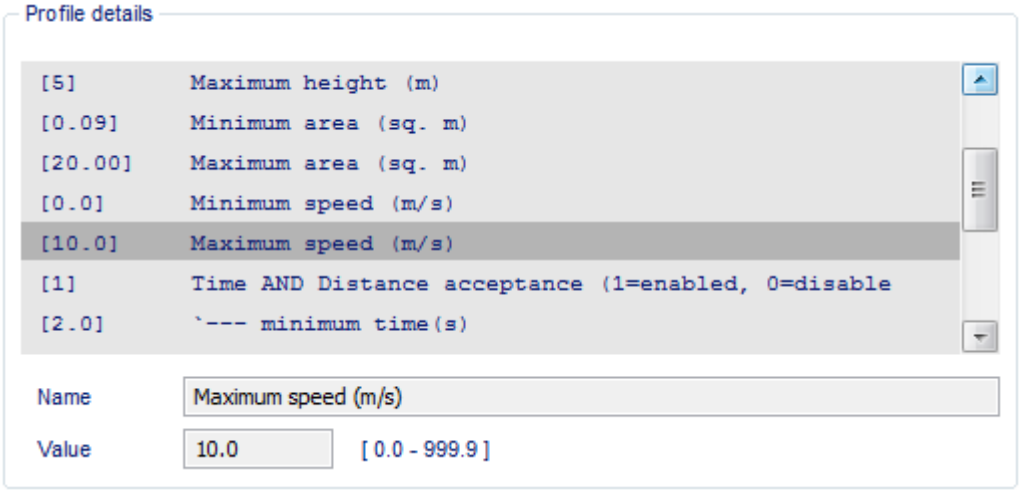
Minimum speed (m/s)

Setting the minimum speed is essential to avoid detection of slow objects. An object will not generate an alarm if its speed is less than the specified value. The value is expressed in metres per second. For detecting humans a typical minimum speed is 2 metres per second.



Maximum speed (m/s)

Setting the maximum speed is essential to avoid detection of rapid objects. An object will not generate an alarm if its speed is higher than the specified value. The value is expressed in metres per second. For detecting humans a typical maximum speed is 10 metres per second (thus avoiding detection of fast cars).

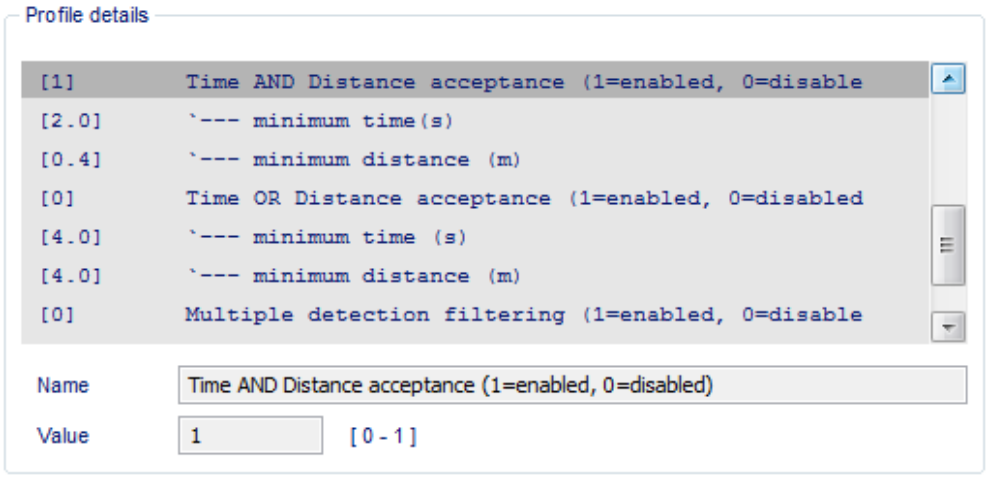


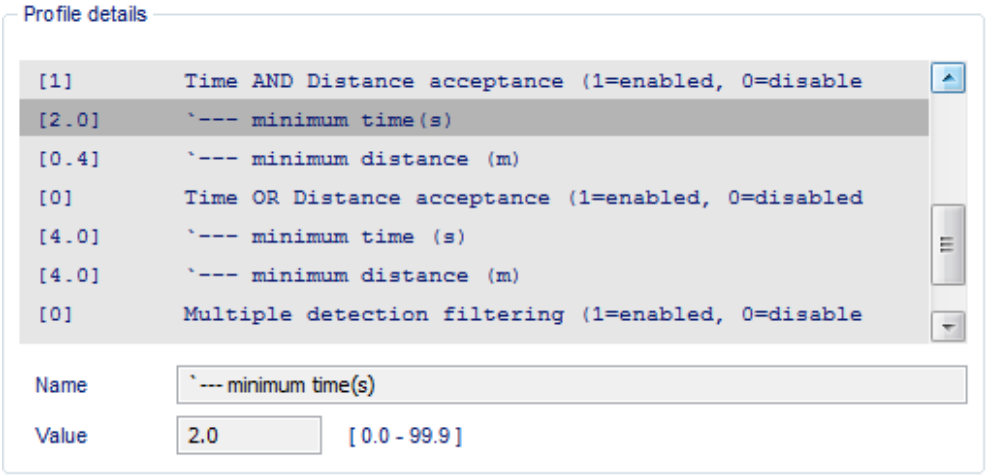
Time AND Distance acceptance (1=enabled, 0=disabled)
---- minimum time (s)
---- minimum distance (m)

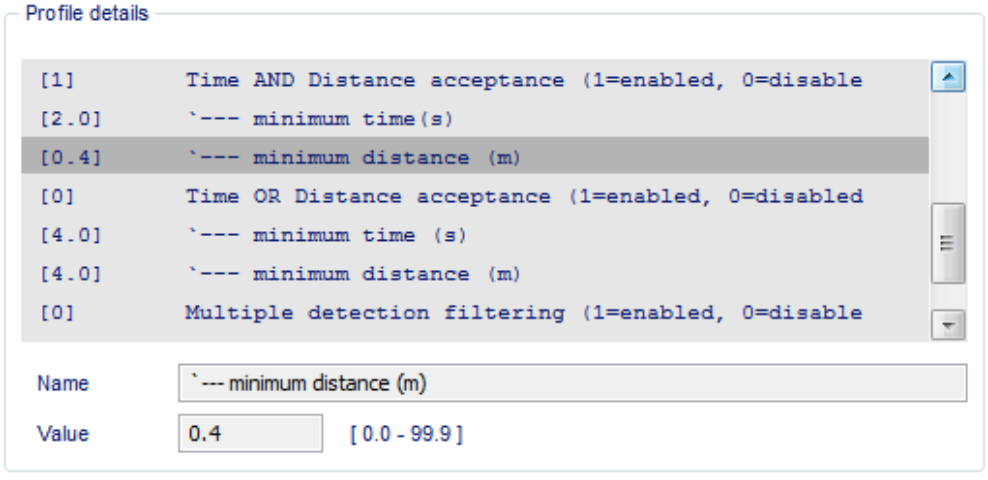
If you enable time AND distance acceptance, an object will only generate an alarm if both conditions underneath have been fulfilled:

- The object has spent more than a specified amount of time in the scene. This value is expressed in seconds.
- The object has travelled more than a specified distance. This value is expressed is metres.

To filter car lightings from a nearby road, use a “minimum time” of the car lightings duration time, with no minimum distance (0 metres). To detect people wandering, use a minimum time of 15 or 30 seconds and a minimum distance of several metres.


Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
Time AND Distance acceptance (1=enabled, 0=disabled)
Value
1
[0 - 1]


Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
`--- minimum time(s)
Value
2.0
[0.0 - 99.9]

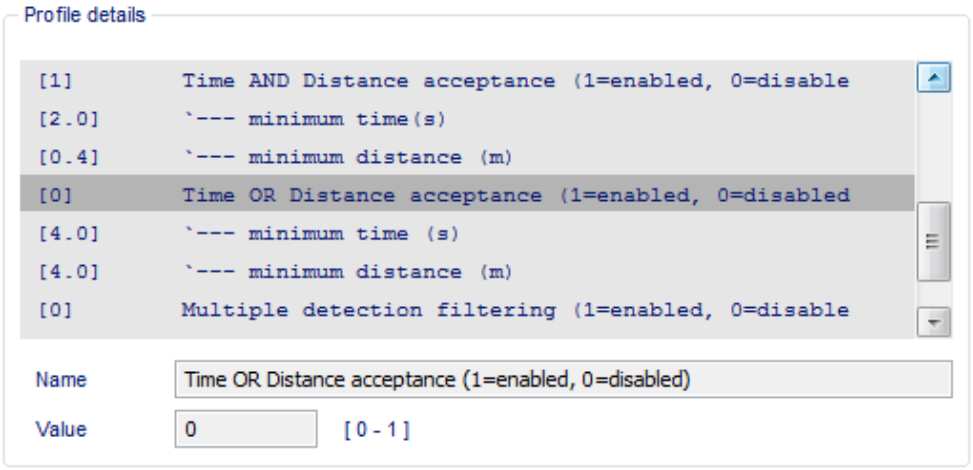

Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
`--- minimum distance (m)
Value
0.4
[0.0 - 99.9]

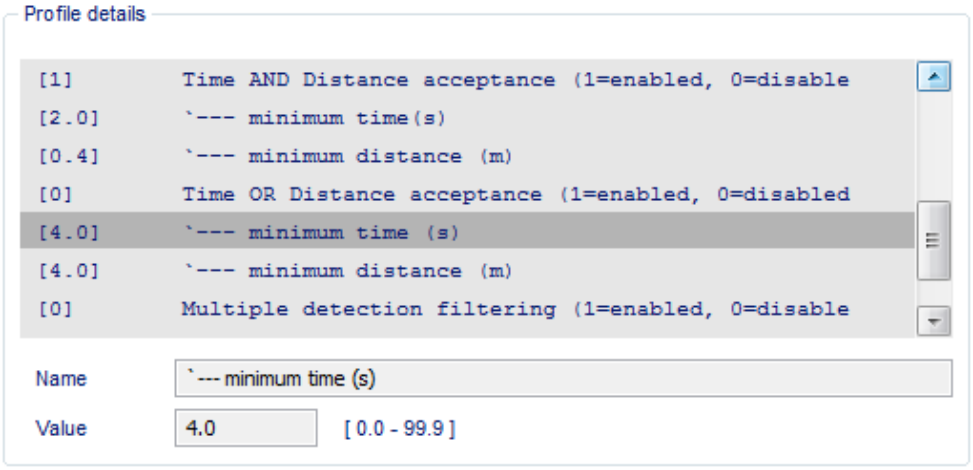
Time OR Distance acceptance (1=enabled, 0=disabled)
---- minimum time (s)
---- minimum distance (m)

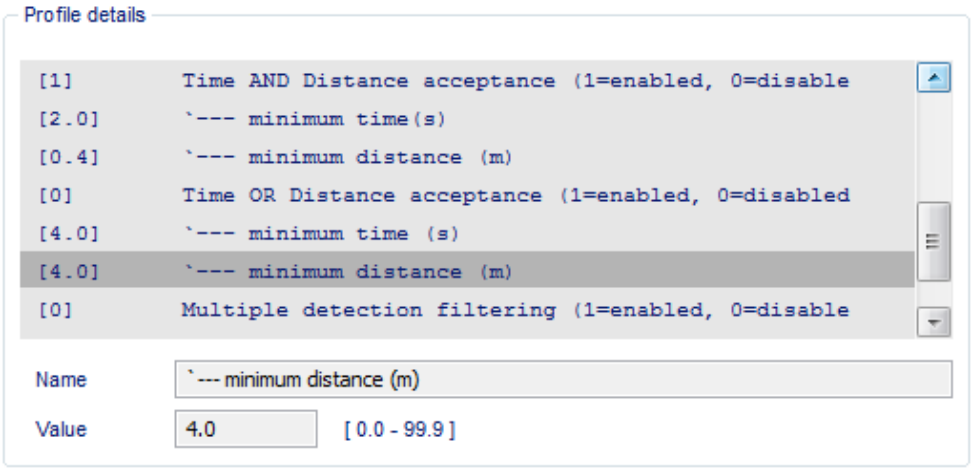
If you enable time OR distance acceptance, an object will generate an alarm if one of the conditions underneath have been fulfilled:

- The object has spent more than a specified amount of time in the scene. This value is expressed in seconds.
- The object has travelled more than a specified distance. This value is expressed is metres.

This setting is useful to detect people trying to approach a secured fence, either by running fast (and thus not staying long enough in the scene) or by crawling slowly (and thus taking a too long time to travel a small distance). Distance and time are very important to determine what settings to use.

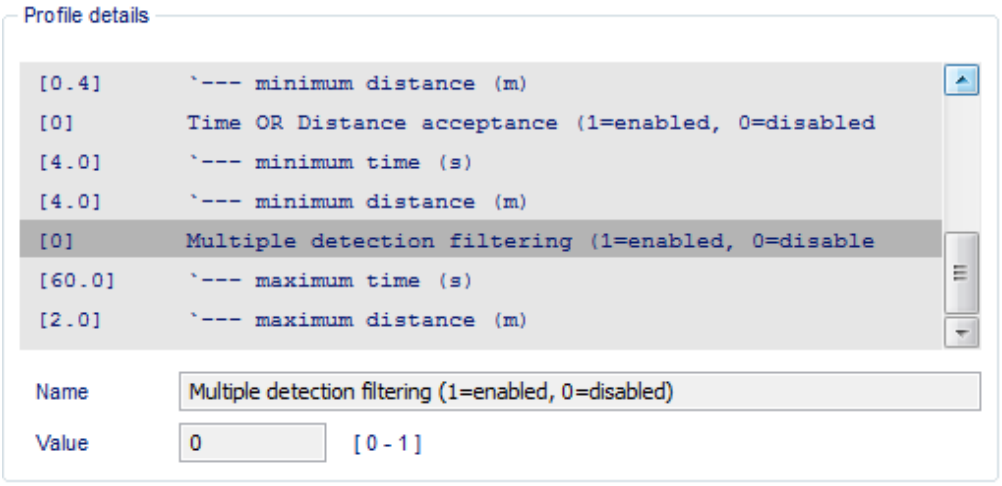

Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
Time OR Distance acceptance (1=enabled, 0=disabled)
Value
0
[0 - 1]

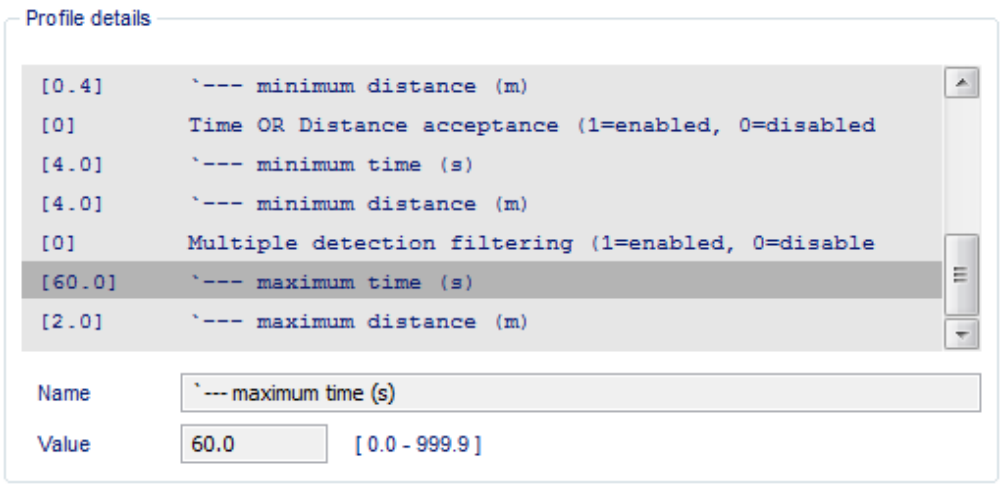

Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
`--- minimum time (s)
Value
4.0
[0.0 - 99.9]

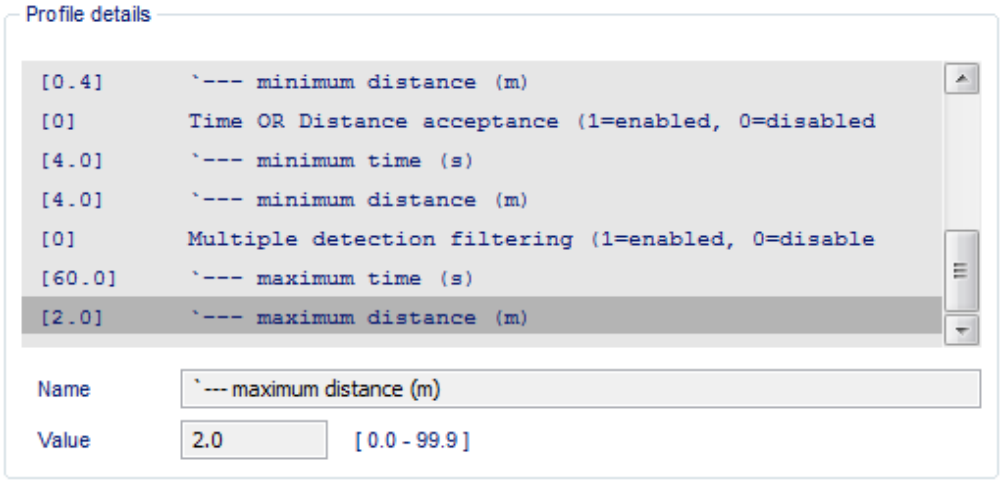

Profile details
[1] Time AND Distance acceptance (1=enabled, 0=disable
[2.0] `--- minimum time(s)
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
Name
`--- minimum distance (m)
Value
4.0
[0.0 - 99.9]

Multiple detection filtering (1=enabled, 0=disabled)
---- maximum time (s)
---- maximum distance (m)

To avoid repetition of alarms in the same area, for a specified duration you can enable the multiple detection filtering. When enabled, no alarm may occur near a previous alarm (how near is specified by the **maximum distance** parameter), for a certain amount of time (how long is specified by the **maximum time** parameter).


Profile details
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
[60.0] `--- maximum time (s)
[2.0] `--- maximum distance (m)
Name
Multiple detection filtering (1=enabled, 0=disabled)
Value
0
[0 - 1]


Profile details
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
[60.0] `--- maximum time (s)
[2.0] `--- maximum distance (m)
Name
`--- maximum time (s)
Value
60.0
[0.0 - 999.9]


Profile details
[0.4] `--- minimum distance (m)
[0] Time OR Distance acceptance (1=enabled, 0=disabled
[4.0] `--- minimum time (s)
[4.0] `--- minimum distance (m)
[0] Multiple detection filtering (1=enabled, 0=disable
[60.0] `--- maximum time (s)
[2.0] `--- maximum distance (m)
Name
`--- maximum distance (m)
Value
2.0
[0.0 - 99.9]

Mind:

If enabled, this parameter may cause a missed detection due to a previous false alarm in the same area.

13.1.4.6.2 Tips for advanced parameters setting

The advanced parameters should only be modified in case the standard settings are not sufficient e.g. rejection of true alarms or acceptance of false alarms.

Ensure that a change in advanced parameters, does not affect the foreseen detection objectives e.g. the intruder could be crawling on the ground, could be a group of persons…

In case of false alarms, determine which parameter(s) filters them out mostly. e.g. the duration is particularly short, the alarm object is huge, …

The advanced parameters concern dimensions, speed, time and distance. Other characteristics could still influence the number of false alarms, e.g. distinguish cars moving slowly from large group of persons is not possible.

To generate an alarm, an object must satisfy all the criteria specified in the advanced parameters during a few seconds AND cross a trigger-line or a detection zone.

13.1.4.6.3 Adding a new detection profile

Enter a name for the new profile and click Add. The new profile will automatically be added to the list. The default settings – identical to the default profile – can now be changed.

13.1.4.7 Save button

Click this button to save the configuration. This will restart the Perimeter Detection with the new parameters.

To store the new settings permanently, open **System > Maintenance > Configuration**, select the desired configuration to overwrite and click **Save**.

13.1.5 Calibration

Click the calibration button (in the Drawing Tools section) to calibrate the scene. Calibration is mandatory as the detection is based on 3D measures.

Calibration
A
B
Unit of measure
Feet
Height of object
5.9
Feet
A
B
Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool.

Select the desired unit of measure (feet or metres) and define the height of the object. Image A shows the image of the object near the camera. Image B shows the image of the object far from the camera. Use a snapshot (from live or recorded images) to draw the measure of the persons.

You can watch live images by clicking the camera button. To start recording the live video images, click the film button. You can play recorded sequences by clicking the camera scope button.

The typical calibration procedure goes as follows:
1) Record a sequence with a person near and far.
2) Play the sequence and pause when the person is near.
3) Take snapshot A and draw its measure.
4) Play the sequence and pause when the person is far.
5) Take snapshot B and draw its measure.
6) Choose unit of measure and height of person.
7) Come back to live stream view.
8) Save.

The recorded sequence is stored on your client PC in the *Documents and Settings* of your user account.

13.1.6 Mask zones

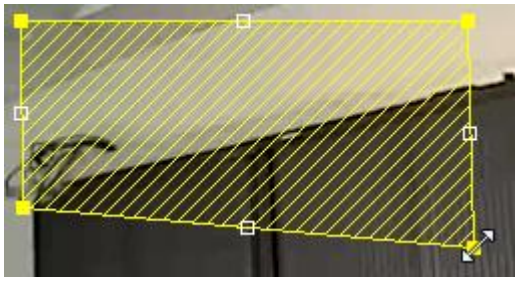
The mask is used to avoid false alarms due to useless parts of the image, e.g. flashing light, on screen display of time, trees, cars … etc.

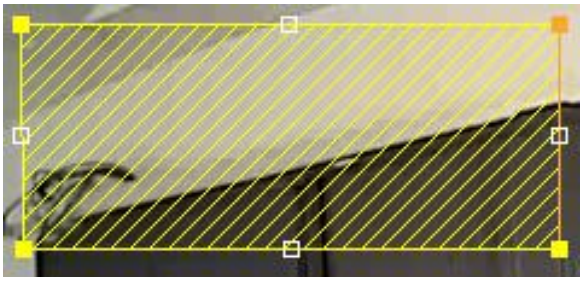
The mask concerns image zones, not ground zones. It should not cover the upper part of the intruder's body anywhere inside the detection zone or anywhere on a trigger line.

Draw a mask area.

Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be hatched with yellow lines, thus creating a yellow mask zone.

You can easily change the form of the polygon by clicking one of the line end points (angles) and drag it to a new position. You can also add a line by deleting one of the lines and automatically start drawing from the last line end point.





Mask areas define the regions that will not be processed by the analytics module. A maximum of 5 polygon areas can be drawn. These areas can overlap.

13.1.7 Detection zones

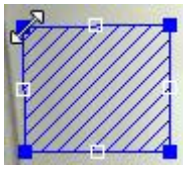
A detection zone is a zone on the ground where intruders should trigger an alarm. The lowest edge of the detection zone should cover the lowest part of the intruder. If the detection zone includes the front part of the scene, the detection zone should come down to the lowest edge of the image.

The alarm is only issued if the person(s) remain(s) at least 2 seconds inside at least one detection zone and moves for at least 0.8 metres (3 ft). In case of an alarm, the concerned detection zone becomes red.

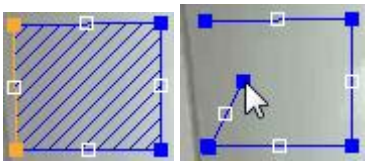
Draw the detection ground zone.

Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be hatched with blue lines, thus creating a blue zone.

You can easily change the form of the polygon by clicking one of the line end points (angles) and drag it to a new position.



You can also add a line by deleting one of the lines and automatically start drawing from the last line end point.



Detection areas define the regions where objects are detected as valid. They must pass the detection criteria while in these areas in order for an alarm to occur. A maximum of 16 polygon areas can be drawn. These areas can overlap.

13.1.8 Trigger lines

A trigger line is a line on the ground that persons should not cross. The lowest point of the trigger line should cover the lowest part of the intruder. If the trigger line concerns the front part of the scene, the trigger line should come down to the lowest edge of the image. Imagine the trigger line as a line painted on the ground that people may not cross.

Draw one or multiple unidirectional trigger lines.

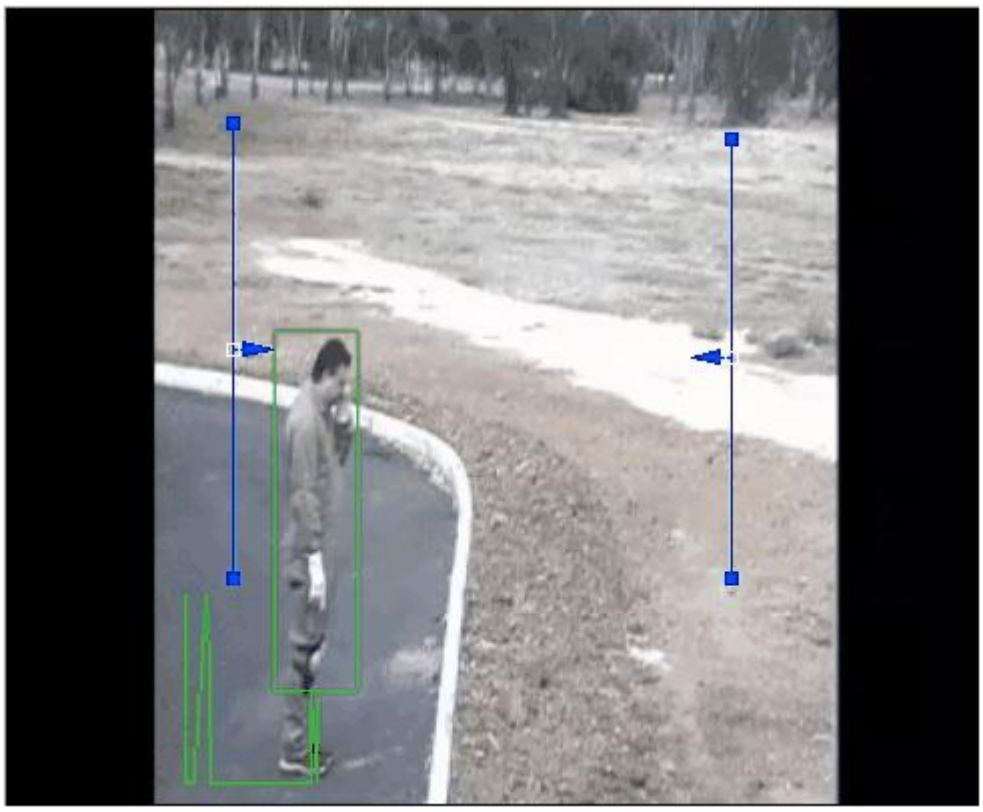
Unidirectional trigger lines are used to trigger an alarm when a person crosses the line in the direction of the arrow. Click the right mouse button to stop drawing trigger lines.

You can easily adapt the position and/or length of the lines by dragging the line ends to a new position.

Draw one or multiple bidirectional trigger lines.

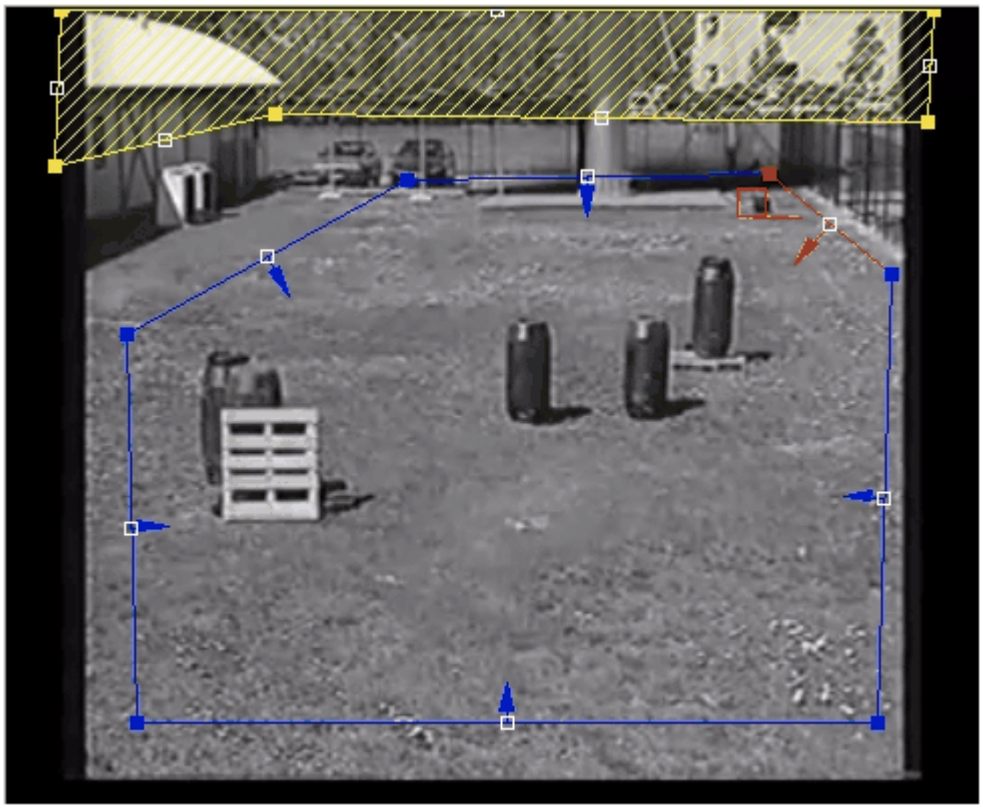
Bidirectional trigger lines are used to trigger an alarm when a person crosses the line in any direction. Click the right mouse button to stop drawing trigger lines.

13.1.8.1 Some examples

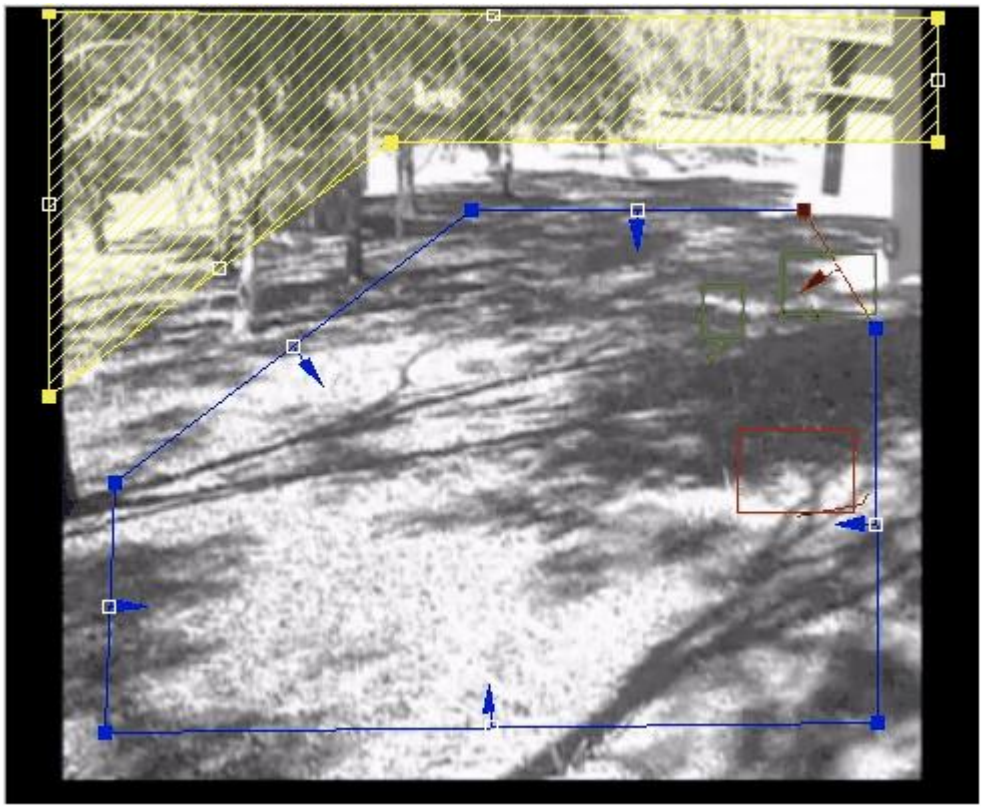


No detection because the intruder's lowest point does not cross the trigger line!

Detection because the intruder's lowest point crosses the trigger line.



Suitable scene: detection of all intruders with almost no false alarms.



Unsuitable scene: many false alarms due to moving shadows.

13.2 FastTrace™ 2 LoiterTrace

LoiterTrace stands for full loitering detection analytics.

13.2.1 About the FastTrace 2 LoiterTrace (Loitering Detection analytic)

The FastTrace 2 Loitering Detection analytic:

- is an image analysis tool able to detect humans remaining a too long time in an indoor scene, even if they remain static for a long time (e.g. sleeping).
- is suited for scenes remaining empty most of the time, not for scenes almost always populated. It can be used in a lobby for example, but not in an airport hall.
- does not depend on the resolution or frame rate of the camera.
- requires a maximum horizontal Field of View (FOV) of 10 m (32.8 ft) and a minimum person's surface of 2% of the image for reliable detection.
- works better if automatic camera adaption (iris, shutter, gain, …) is slow or disabled.
- has 3 sensitivity levels:
  - normal (= default)
  - low (for avoiding false alarms from outdoor influence, static changes, … etc.)
  - high (for avoiding missed detections)
- could mask parts of the image to avoid false alarms due to flashing light, trees, cars, on screen display of time, … etc.
- uses *Ground Region of Interest*: any object whose lowest point (= ground position) is outside of the GROI will not trigger a loitering detection. It is advised to use a larger GROI zone than the real ground zone surveyed. It is also advised to include the lower edge of the image to make sure that persons at the bottom of the image are not excluded from detection.

13.2.2 Scope

The FastTrace 2 Loitering Detection analytic is an image analysis tool able to detect human(s) remaining a too long time in an indoor scene.

The Loitering Detection uses advanced algorithms to maximize target detection and tracking. It is able to detect loitering persons even if they remain static for a long time (like when the person is sleeping).

The Loitering Detection is suited for (parts of) scenes remaining empty most of the time. It is absolutely not suited if the scene is almost always populated. It can be used for a lobby, but certainly not for a crowded airport hall.

13.2.3 Camera

13.2.3.1 Resolution and frame rate

Whatever the resolution of the camera, the system is providing the analytics with CIF images at a frame rate of 5 frames per second. The resolution and frame rate used for monitoring or continuous/event recording have no influence on the Loitering Detection analytic.

13.2.3.2 Field of View (FOV)

If a person is loitering too far from the camera, it cannot be detected or continuously tracked. The width of a person should be more than 5% of the width of the image, this corresponds to a horizontal FOV of about 10 metres (32.8 ft).

person is too far (3mm / 85mm < 5%)

13.2.3.3 Position

If a too large part of a person is hidden from the camera, or masked, the person cannot be detected. The image surface of the person should be at least 2% of the image.

too small part of the person
(person surface /image surface = 9x4 mm² / 85x38 mm² < 2%)

13.2.3.4 Scene illumination

The software is not able to detect objects in a too badly illuminated scene. If the bad illumination concerns a part of the scene, the tracking of the objects could stop within part of the scene.

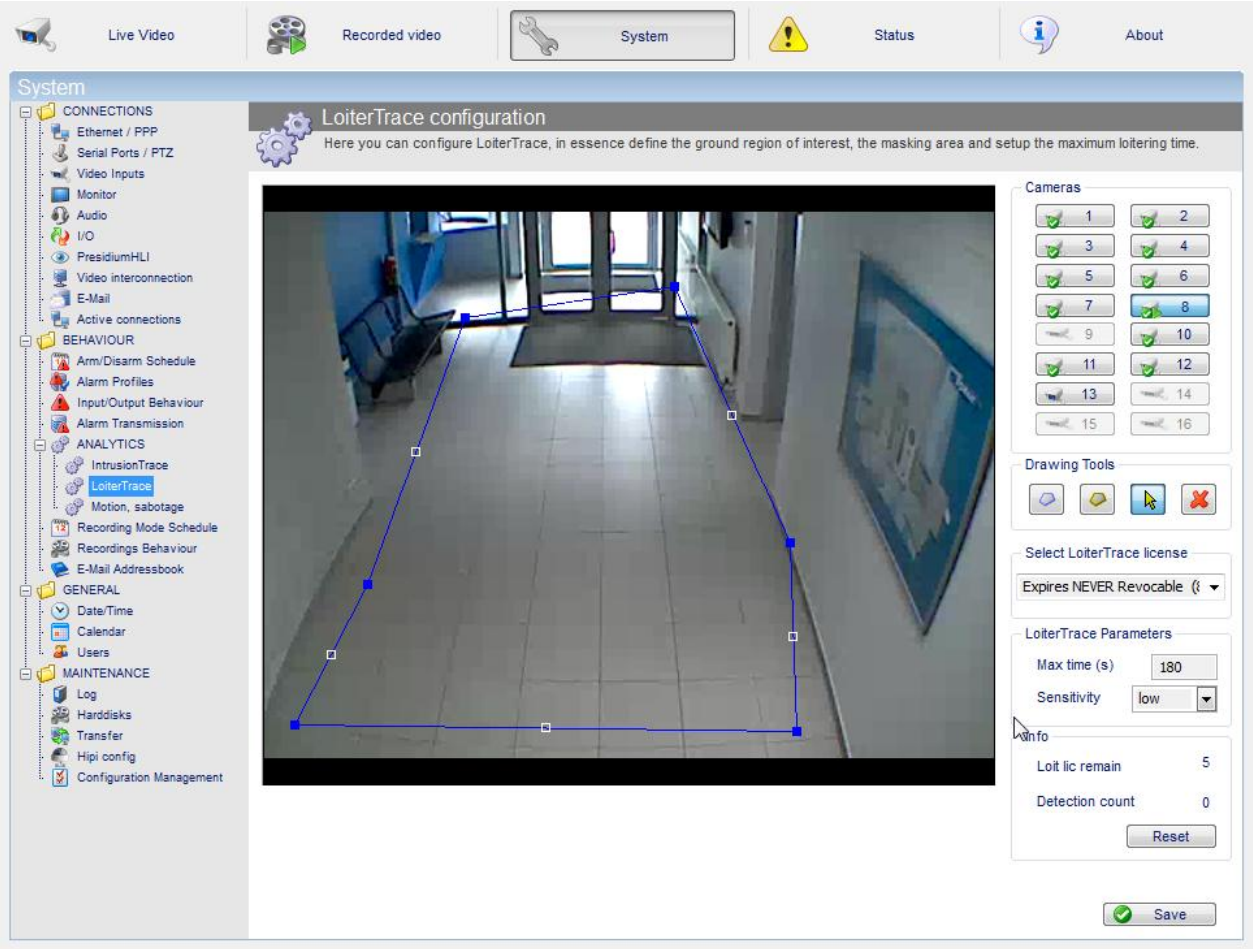
13.2.3.5 Automatic camera adaption

It is recommended to disable automatic camera adaptation (iris, shutter, gain, …) or to use slow adaptation settings.

13.2.4 Configuration

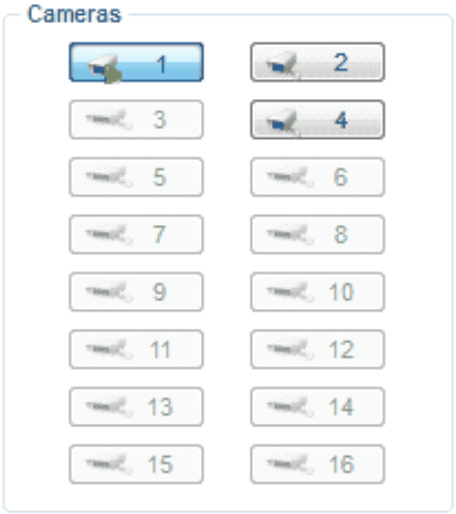
13.2.4.1 Loitering configuration interface

In the FastTrace 2 Client, open **System > Behaviour > Analytics > LoiterTrace**.



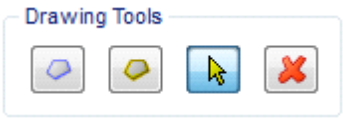
13.2.4.2 Cameras section

Select the desired camera you want to configure loitering detection for. Only one camera at the same time can be selected.



13.2.4.3 Drawing Tools section

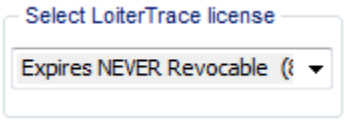
You can add several loitering detections settings to the image. Use the drawing tools to add these settings. All necessary information about the tools is shown under the image when you click the button.



Icon	Description
	Draw the detection ground region. Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be a blue zone. Ground regions define the regions where objects are detected as valid. They must pass the detection criteria while in these areas in order for an alarm to occur. A maximum of 5 polygon areas can be drawn. These areas can overlap.
	Draw a mask area. Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be creating a yellow mask zone. Mask areas define the regions that will not be processed by the analytics module. A maximum of 5 polygon areas can be drawn. These areas can overlap.
	Select objects by clicking them.
	Delete the selected object.

13.2.4.4 Select LoiterTrace license

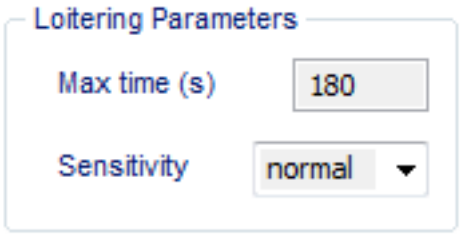
In the *Select LoiterTrace license* section, you need to select what license you will use for this specific camera.



If you have no licenses available you either need to buy extra credits or transfer a license. See the *Application License Guide* for further information.

13.2.4.5 Loitering parameters

In the “Loitering Parameters” section you can define the maximum time (value in seconds) a person can stay in the ground zone(s). If the person’s presence in a zone supersedes this value, a loiter alarm is triggered. It is recommended to enter a value higher than 20.



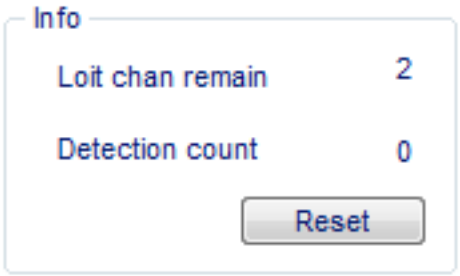
You can also determine how sensitive the detection should be to objects remaining static for a long time:

- Low: the max staticity duration is fixed to 10 seconds.
  > No loss of track of static objects if they move regularly;
  > Should be used if there are too many false alarms (due to high outdoor influence, doors, …).
- Normal: the max staticity duration is the half of the max loitering time. This is the default sensitivity level.
  > No loss of track of static objects if they move sometimes.
- High: the max staticity duration is the max loitering time.
  > No loss of track of static objects, even if they do not move during the max loitering time;
  > Should be used if there are too many missed detections (e.g. with sitting or sleeping persons).

13.2.4.6 Info section

In the *Info* section you can see how many “loitering channels remain”. This indicates the number of remaining loitering detection licenses (i.e. the subtraction between the total number of licenses and the number of used licenses).

The “Detection count” indicates the number of detections while the configuration was running. You can reset the detection count by clicking **Reset**.



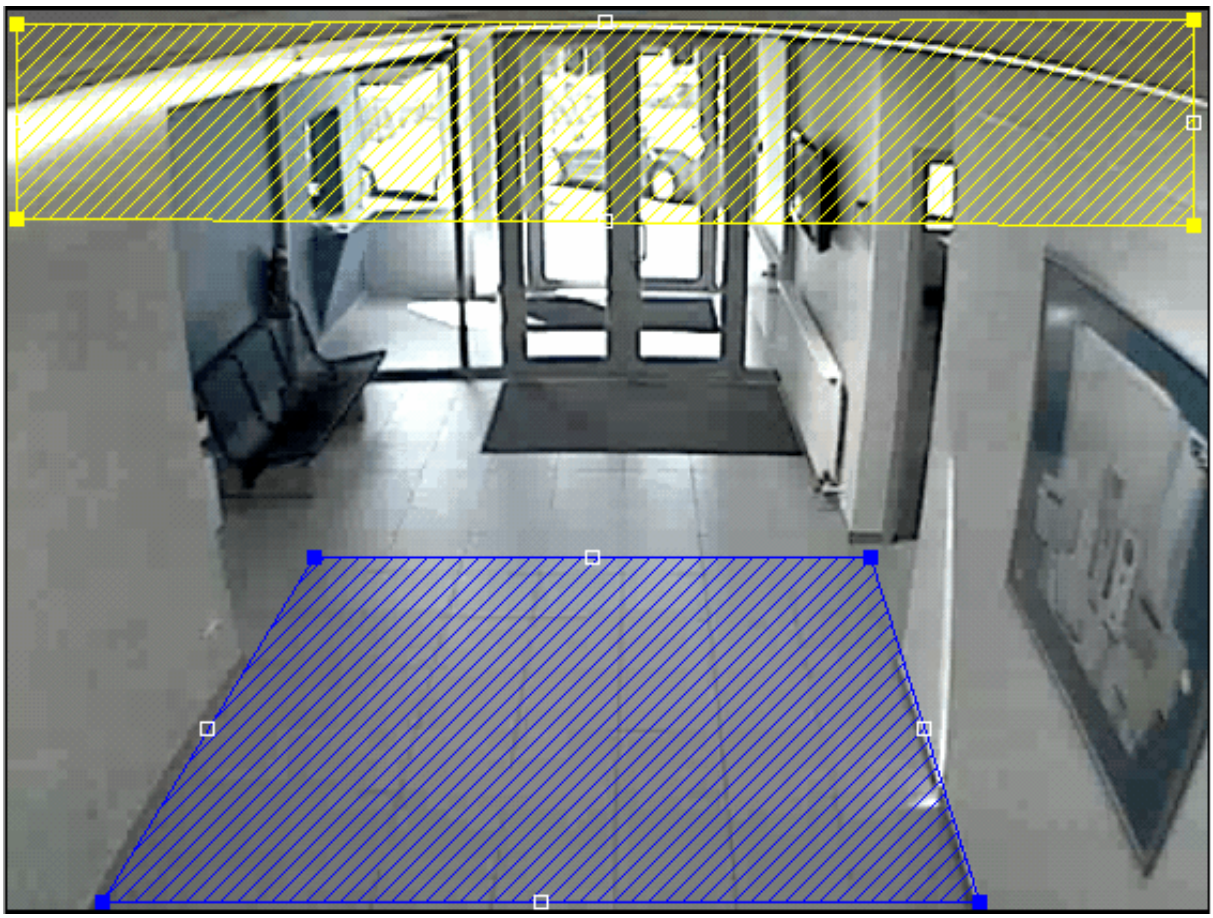
13.2.4.7 Save button

Click this button to save the configuration. This will restart the Loitering Detection with the new parameters.

To store the new settings permanently, open **System > Maintenance > Configuration**, select the desired configuration to overwrite and click **Save**.

13.2.5 Mask zones

The mask is used to avoid false alarms due to useless parts of the image, e.g. flashing light, on screen display of time, outside influence … etc.

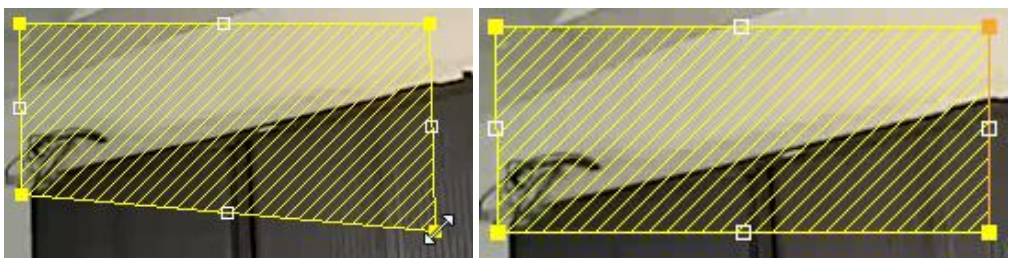


The mask concerns image zones, not ground zones. It should not cover the upper part of the intruder's body anywhere inside the *Ground Region of Interest*.

Draw a mask area.

Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be hatched with yellow lines, thus creating a yellow mask zone.

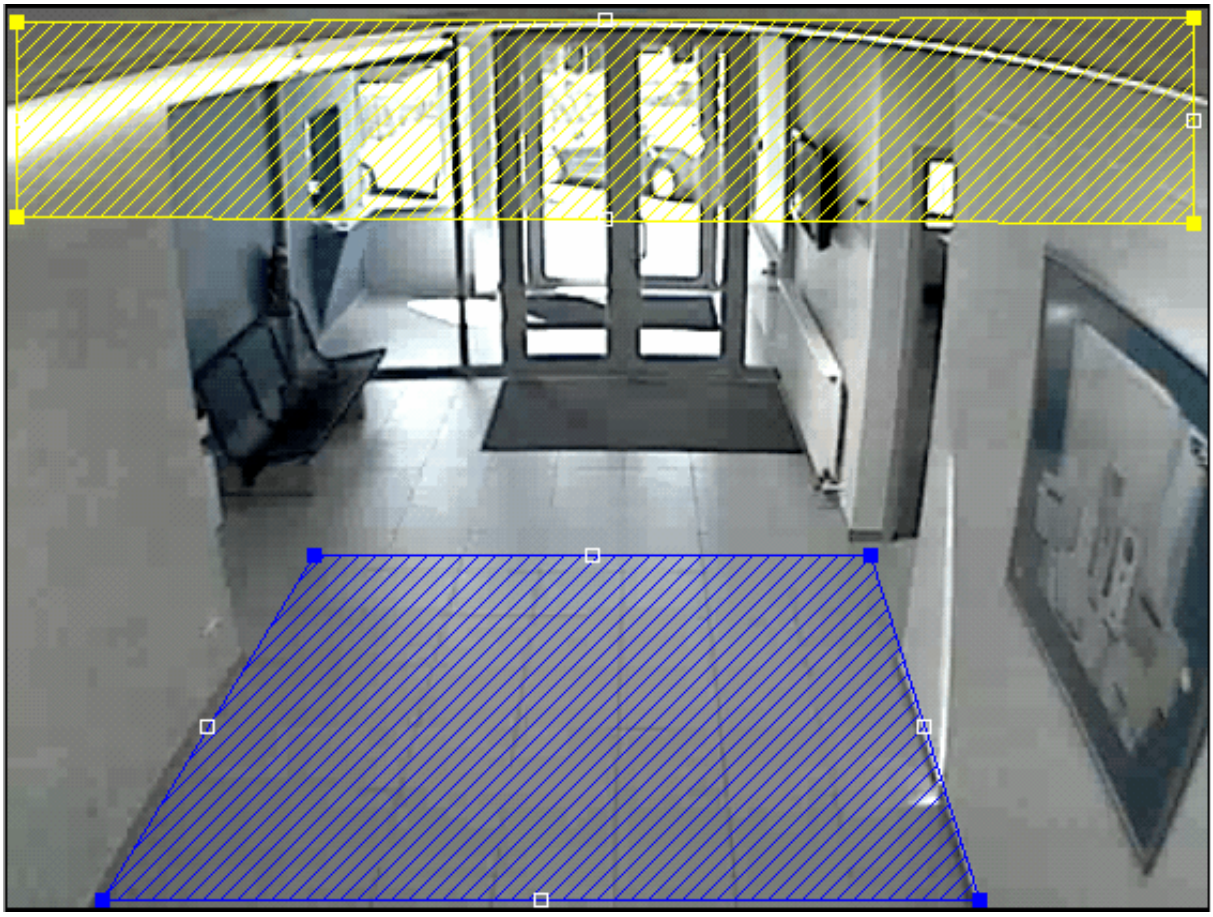
You can easily change the form of the polygon by clicking one of the line end points (angles) and drag it to a new position. You can also add a line by deleting one of the lines and automatically start drawing from the last line end point.



Mask areas define the regions that will not be processed by the analytics module. A maximum of 5 polygon areas can be drawn. These areas can overlap.

13.2.6 Detection zones

A *Ground Region of Interest* (GROI) is a zone on the ground where loitering should trigger an alarm. The lowest edge of the detection zone should cover the lowest part of the intruder. If the detection zone includes the front part of the scene, the detection zone should come down to the lowest edge of the image.

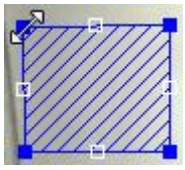


Any object whose lowest point (= ground position) is outside the GROI cannot trigger a loitering detection and so no alarm will be given. It is advised to use a larger zone than the real ground zone. It is also advised to include the lower edge of the image to make sure that object present at the bottom of the image are not excluded from detection.

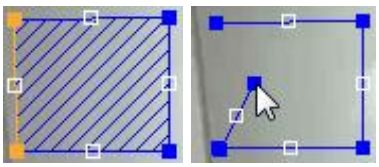
Draw the detection ground region.

Click the left mouse button each time you want to make an angle. When closing the lines in the object, the area will be a blue zone.

You can easily change the form of the polygon by clicking one of the line end points (angles) and drag it to a new position.



You can also add a line by deleting one of the lines and automatically start drawing from the last line end point.



Ground regions define the regions where objects are detected as valid. They must pass the detection criteria while in these areas in order for an alarm to occur. A maximum of 5 polygon areas can be drawn. These areas can overlap.

13.2.6.1 Samples

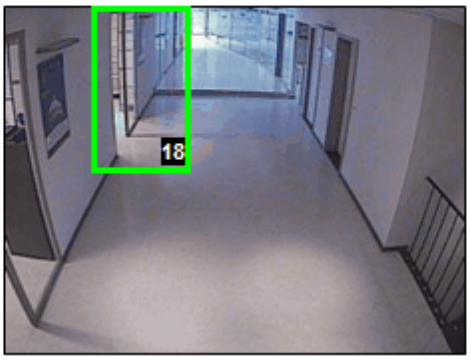
GROI (blue zone) including lowest edge: detects persons coming from below

GROI (blue zone) not including lowest edge: does not detect persons coming from below

Crossing persons

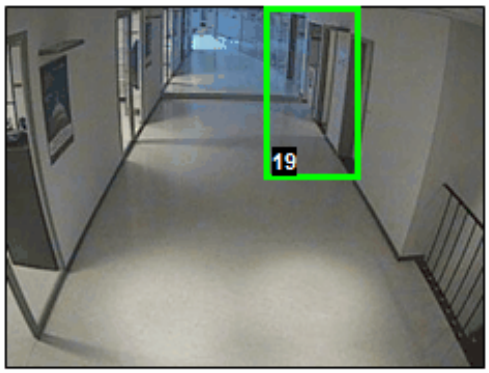
In case of persons crossing each other in the image, the software cumulates the loitering time of the highest time indication to each of them.

Local Illumination changes
An illumination change, e.g. a large light spots, could cause an object detection for some seconds, or for a longer time, depending on the "sensitivity" parameter.



Global illumination changes
A global illumination change, e.g. the light is set off or on, could also cause an object detection for a some seconds, or for a longer time, depending on the "sensitivity" parameter. If the change occurs while a person is loitering, the person's loitering time will then restart at 0" as soon as the person moves again.

Static objects
If static objects are added or removed, or if the scene changes e.g. a door remains open, they will cause an object detection during some seconds. The higher the "sensitivity", the longer the object detection time, up to the maximum loitering time when a HIGH "sensitivity" is set.



Static persons

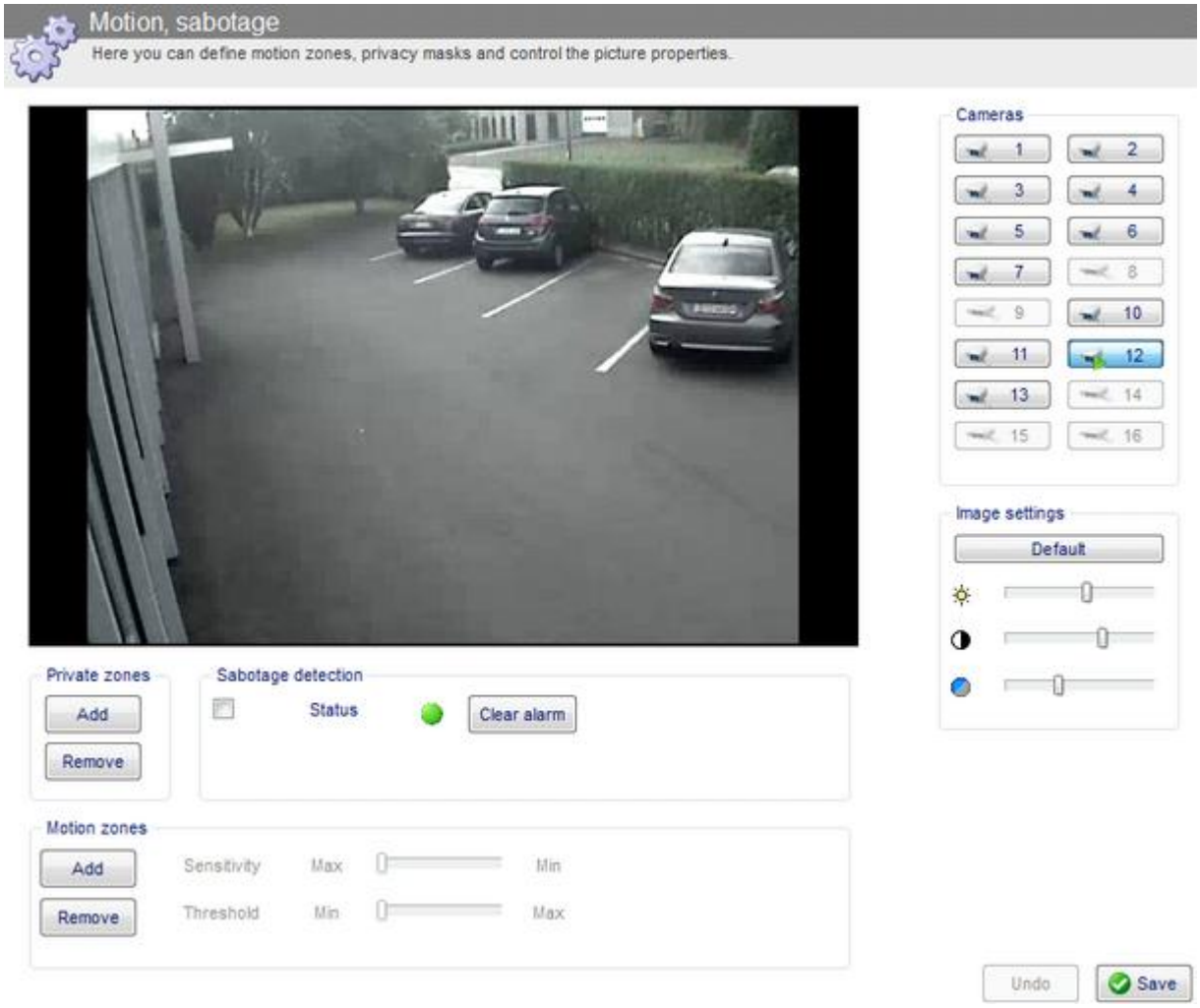
The software is able to detect loitering persons even if they remain static for a a long time (e.g. sleeping). If other persons are crossing the scene while the person is static, the behaviour of the system will depend on the "sensitivity" parameter:

- low sensitivity means that the static person is no longer followed after 10 seconds;
- normal sensitivity means that the static person is no longer followed after 50% of the max time;
- high sensitivity means that the persons will always be followed, even when static for the full period of time. This will always generate an alarm when the maximum time is reached.

13.3 Motion & Sabotage

13.3.1 Motion Detection Interface

Open the *Motion, sabotage* window via **System > Behaviour > Analytics > Motion, sabotage**.

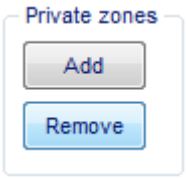


Select a camera.

13.3.2 Private zones

Outdoor security cameras may unintentionally look into neighbourhood residences. To respect their privacy, these parts of the picture can be masked.

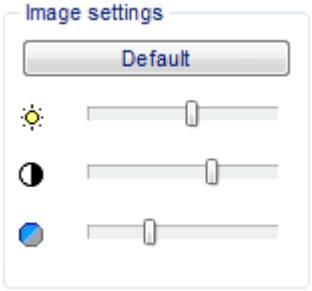
Click **Add** in de section *Private zones*.



On the image a black rectangle will appear in the upper left corner.

You can adjust the size and position of the rectangle to make sure the correct zone is masked.

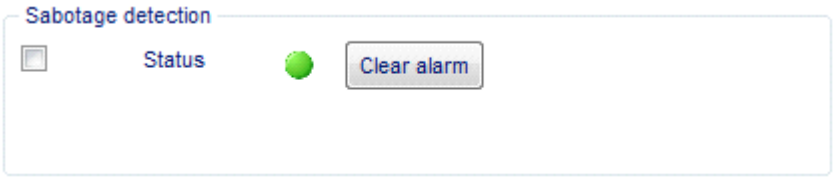
Up to 4 zones can be masked.
If the black box is not clearly visible in the image, adjust the brightness and/or contrast of the image. You can use the sliders in the *Image settings* sections to do this.



Click **Save** to apply the new settings.

13.3.3 Sabotage detection

When a device is being tampered with, the sabotage detection will generate a so-called tamper alarm. This can be activated per camera. In order to do so, tick the option in the section “Sabotage detection”.



The following actions with the camera will result in a tamper alarm:
1. the lens is covered
2. the position of the camera is altered
3. the zoom of the camera image is changed
4. the focus of the camera image is changed

When a tamper alarm is being generated on a certain camera, the green colour for status will change to red. The tamper alarm on the camera should be cleared manually. To clear the tamper alarm on the camera, click **Clear alarm**.

Click **Save** to apply the new settings.

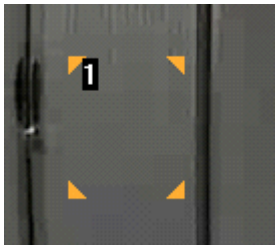
13.3.4 Motion detection

Per camera up to 4 motion detection fields can be defined. Detection of a moving object within this field will trigger an alarm that can be transmitted to the CMS. Motion detection can also be used to start a new recording.

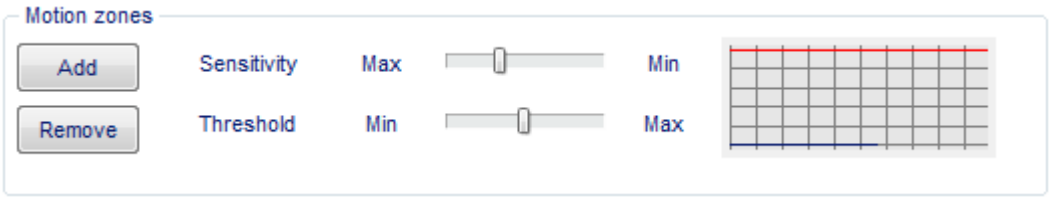
In the section *Motion detection* click **Add**.

Four blue corners (forming a square) appear on the video image. The form also gets a number (1 to 4). You can adjust the size and position of the form by clicking the form with the left mouse button.

When you select (= click) the blue square, the colour changes to orange. Now you can adapt the motion detection settings.



For **analogue cameras** you can adjust the sensitivity and the threshold.



- Sensitivity: sets the level of luminance change required to detect motion.
- Threshold: sets the number of pixels that should change in order to detect motion. This parameter sets the size of the objects that should be detected. It allows suppressing false events such as small animals passing by.

In most cases, sensitivity and threshold have to be adjusted by trial.

For **IP cameras** you can adjust time and minimum object size:

- Time: sets a delay. Minimal delay means that the motion is detected immediately when an object starts moving in the detection zone; maximal delay means that the motion is detected when the object is moving inside the detection zone for some time.
- Min Object Size: sets the object size relative to the region size. Minimal object size means that even very small objects (e.g. small animals like cats and dogs) will trigger motion detection; maximal object size means that only very large objects cause motion detection alarm.

It is recommended to test out the settings to obtain the best result!

When motion is detected in the detection zone, the colour of the form corners will turn green.

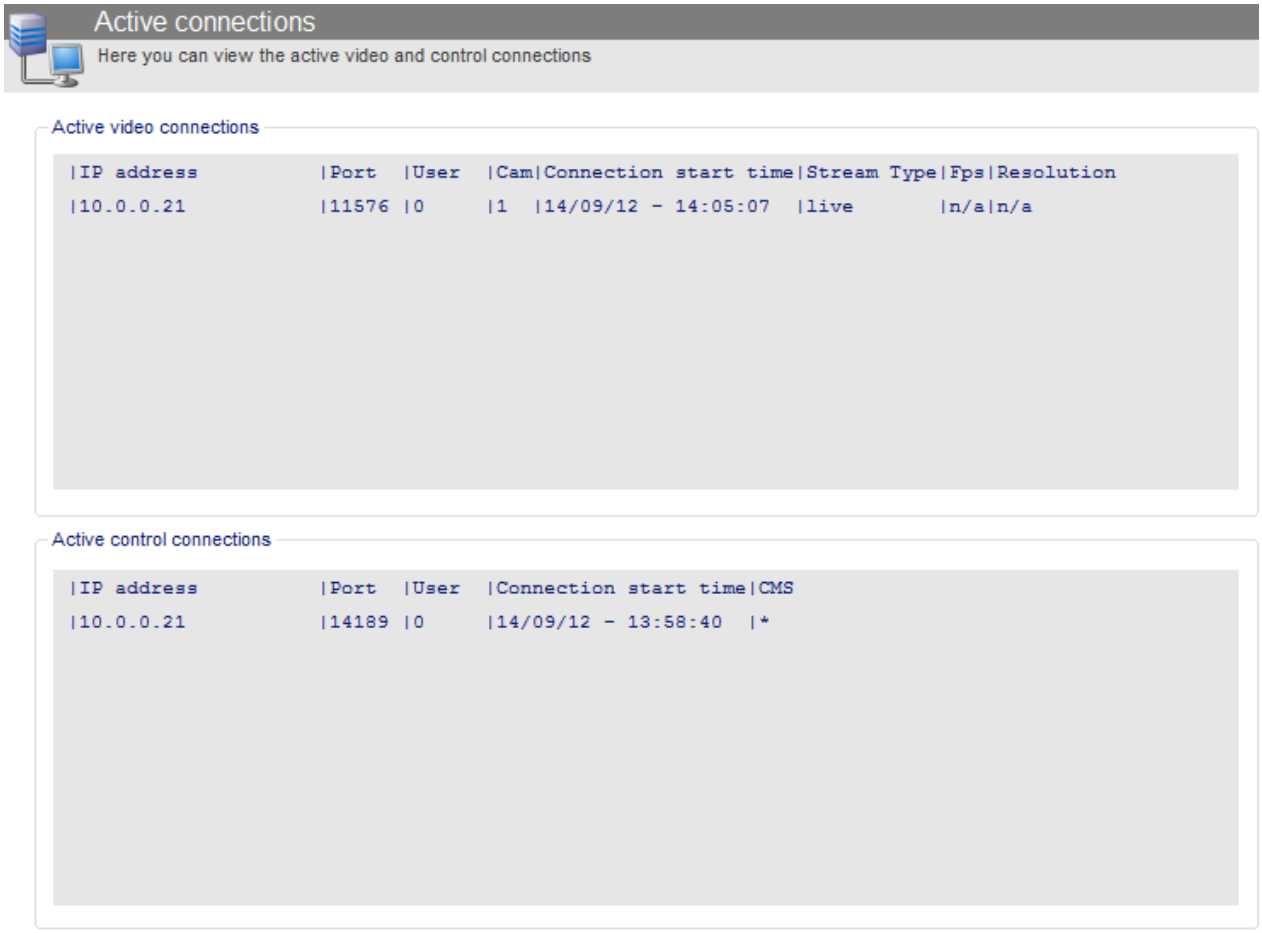
Click **Save** to apply the new settings.

To remove a motion detection zone, select the detection zone and click **Remove**.

14 Active connections

The *Active connections* window has been added to show the active client protocol connections and the active RTSP connection.

Open the *Active connections* window **via System > Connections > Active connections**.

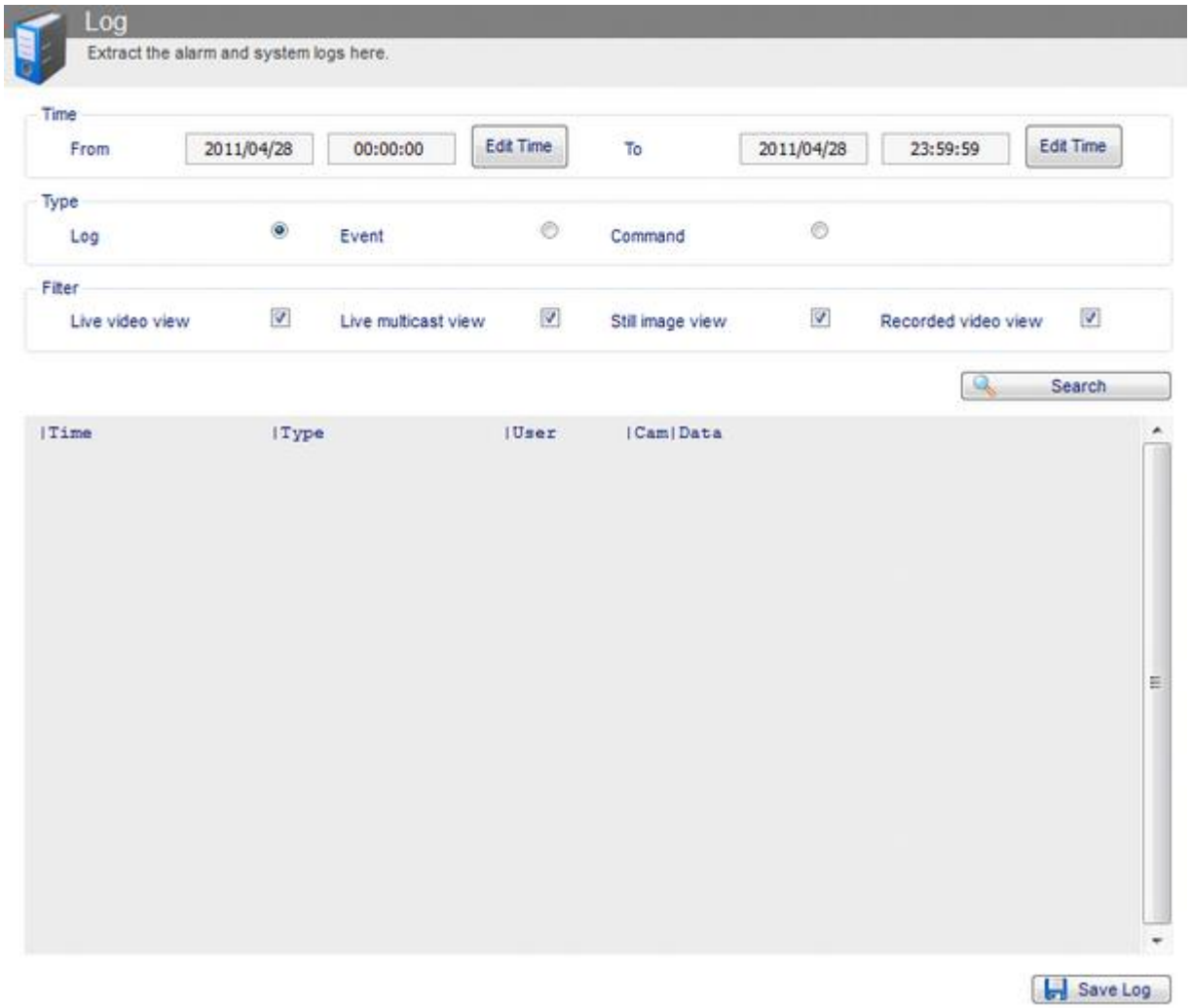

Active connections
Here you can view the active video and control connections
Active video connections
|IP address |Port |User |Cam|Connection start time|Stream Type|Fps|Resolution
|10.0.0.21 |11576 |0 |1 |14/09/12 - 14:05:07 |live |n/a|n/a
Active control connections
|IP address |Port |User |Connection start time|CMS
|10.0.0.21 |14189 |0 |14/09/12 - 13:58:40 |*

The upper section displays the active video connections (=active RTSP connection). The lower section displays the Active control connections (=active client protocol connections).

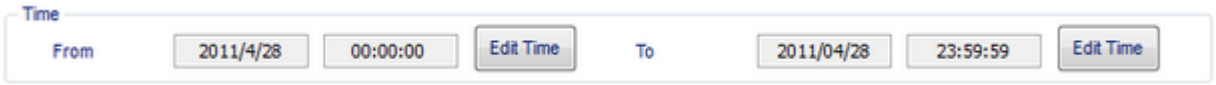
15 Log

Local legal requirements (variable and depending on state and region) may stipulate that a video system should keep a logbook (e.g. the Law Sarkozy in France). This logbook should register all user interventions and events.

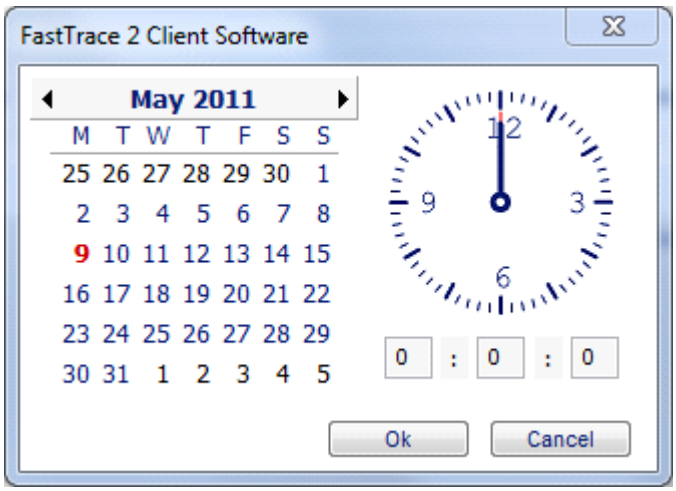
Open the “Log” window via **System > Maintenance > Log**.



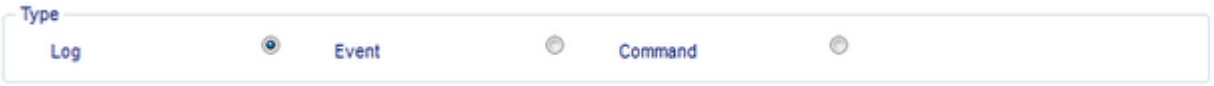
Set the desired time frame.



You can manually type the dates and time indications or click the ‘Edit Time’ button to get this popup window:

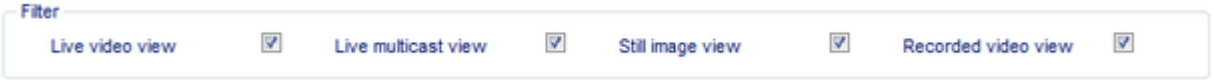


Select the desired type.



You can only select one option: log, event or command.

If you choose ***log*** as type, you can also tick the views you would like to search in the “Filter” section.



Live video view	This option shows the users that have watched live video images.
Live multicast view	This option shows the users that have watched the multicast stream.
Still image view	This option shows the users that have taken snapshot pictures.
Recorded video view	This option shows the users that have downloaded video recordings.

If you choose ***event*** as type, all events that have been generated on the FastTrace 2 video system (e.g. motion detection, inputs, outputs, …) will be displayed.

If you choose ***command*** as type, all commands that have been executed by the users (e.g. connections, change of configuration, …) will be displayed.

Mind:

The log is limited to 100,000 events per type (log, event or command) and has a time period limit of 6 months.

15.1 Example of a Log record

Time	Type	User	Cam	Data
2011/04/28 09:42:14	Still image view	00	01	2011/04/28 06:05:19
2011/04/28 09:41:31	Recorded video view	00	01	2011/04/28 06:05:16 2011/04/28 23:59:59
2011/04/28 09:41:25	Still image view	00	01	2011/04/28 06:05:16
2011/04/28 09:41:24	Still image view	00	01	2011/04/28 06:05:45
2011/04/28 09:40:43	Recorded video view	00	01	2011/04/28 06:04:40 2011/04/28 23:59:59
2011/04/28 09:40:32	Still image view	00	01	2011/04/28 06:05:28
2011/04/28 09:39:47	Recorded video view	00	01	2011/04/28 06:05:32 2011/04/28 23:59:59
2011/04/28 09:39:34	Still image view	00	01	2011/04/28 09:38:15
2011/04/28 09:34:08	Still image view	00	01	2011/04/28 06:05:24
2011/04/28 09:32:44	Still image view	00	01	2011/04/28 06:05:46
2011/04/28 08:47:07	Still image view	00	01	2011/04/27 17:11:03
2011/04/27 09:07:27	Live video view	00	01	
2011/04/27 09:07:26	Live video view	00	02	

↑	↑	↑	↑	↑
Time of intervention	Type of intervention	User of intervention	Camera of intervention	Additional information (e.g. moment of the still image)

15.2 Example of an Event record

Time	Input/Output Behaviour	E	T	ATX	Alarm Time	Alarm
2012/07/27 08:39:03	I0214 - RECORDING MATCH	+	S			
2012/07/27 08:39:03	I0200 - REMOTE CONNECTION	+	S			
2012/07/27 08:26:06	I0214 - RECORDING MATCH	+	S			
2012/07/27 08:26:06	I1034 - CAM01 MOTION1	+	Q			
2012/07/27 08:24:59	I0214 - RECORDING MATCH	+	S			
2012/07/27 08:24:59	I1034 - CAM01 MOTION1	+	Q			
2012/07/27 08:24:27	I0214 - RECORDING MATCH	+	S			

↑	↑	↑	↑	↑
Time of intervention	Identification of intervention	Start or end of intervention	Type of event: - L=Live - Q=Quad - D=Duress - S=Systeem	Additional information on the alarm

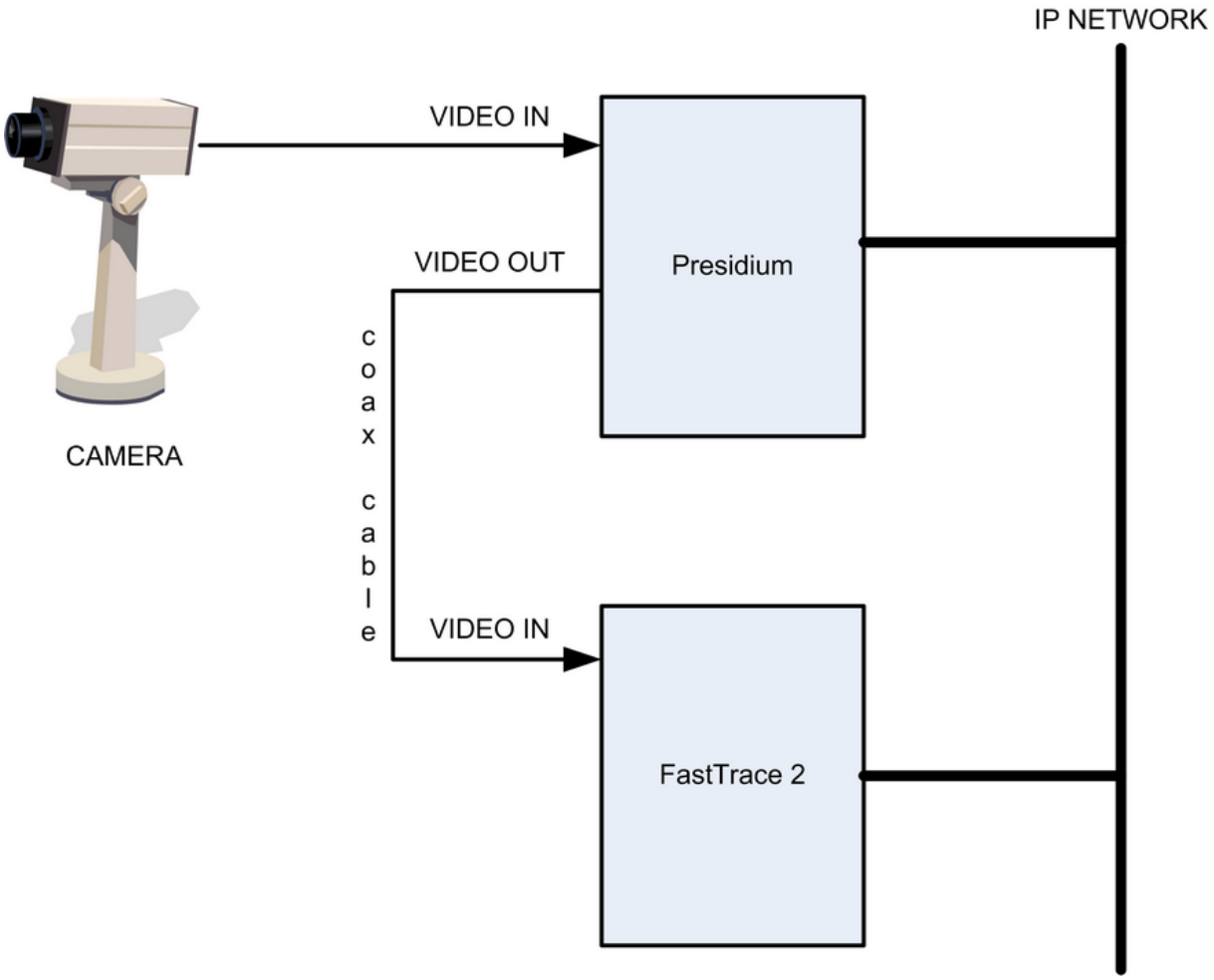
15.3 Example of a Command record

Time	Id	Group	Command	Data
2011/04/28 09:39:30	C01	transfer	download	user data
2011/04/28 09:39:30	C01	login	user	(00) => authorized
2011/04/28 09:39:30	C01	connection	open	(10.0.0.236)
2011/04/28 09:35:32	C11	system	reboot	
2011/04/28 09:33:59	C11	transfer	download	user data
2011/04/28 09:33:59	C11	login	user	(00) => authorized
2011/04/28 09:33:59	C11	connection	open	(10.0.0.236)
2011/04/28 09:33:55	C10	connection	closed	(10.0.0.236)
↑	↑		↑	↑
Time of intervention	Event identification. * - C = client session - T = telnet session		Executed command	Additional information (e.g. IP adres)

** All commands within the same session will have the same ID. The number that is attributed to the command log ID is increased with every connection that is made. When the number 64 is reached, the next number will again be 1.*

16 Presidium High Level Interface

The “PresidiumHLI” window allows to associate video outputs from a Presidium to the FastTrace 2 inputs. The video outputs of the Presidum system can be connected by means of a coax cable to the inputs of a FastTrace 2 video system for further analysis and recording. That way it is possible to transmit alarms from the Presidium to the FastTrace 2 over the IP network.



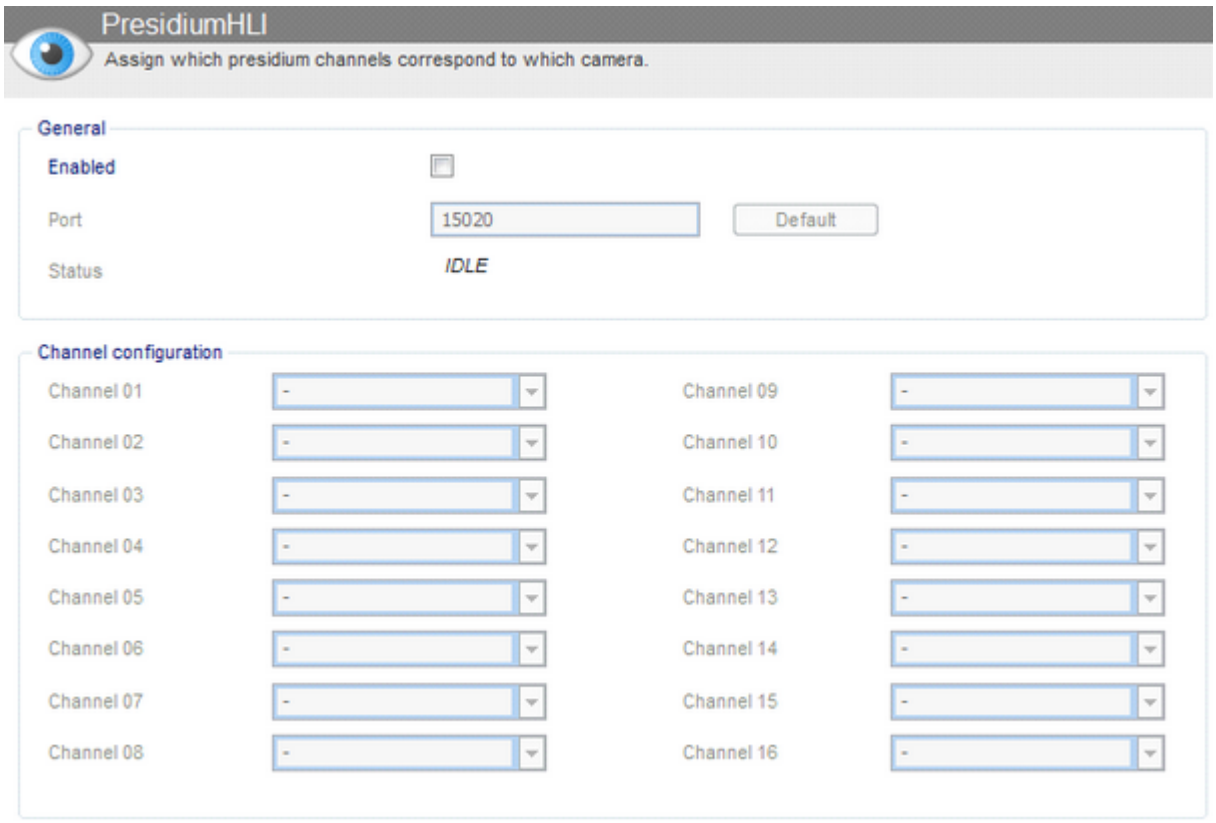
To set up the Presidium connection, open **System > PresidiumHLI**.

Tick the option “Enabled”. Also enter the IP port through which the Presidium can communicate to the FastTrace 2 Server. Only the IP port needs to be defined in the FastTrace 2 video system. All other communication settings need to be programmed on the Presidium itself.

The connection to a Presidium can activate following events on the FastTrace 2:

- I0070 PRESIDIUM FAULT: the Presidium reports a high temperature or general fault, or the FastTrace 2 detects a wrong IP port;
- I0071 PRESIDIUM PRESENCE FAULT: no communication with the Presidium;
- I1024 CAM01 NO VIDEO: video signal is missing (detected by the Presidium)
  I1025 CAM01 CONTRAST ERROR: camera lens is covered (detected by the Presidium)
  I1033 CAM01 PRESIDIUM DET: alarm on camera (detected by the Presidium);
  ➞ These alarm messages can be transmitted per camera (hence the mentioning of the camera in the examples above).

In the “Channel configuration” section you need to specify what video outputs of the Presidium have been connected to each FastTrace 2 input.



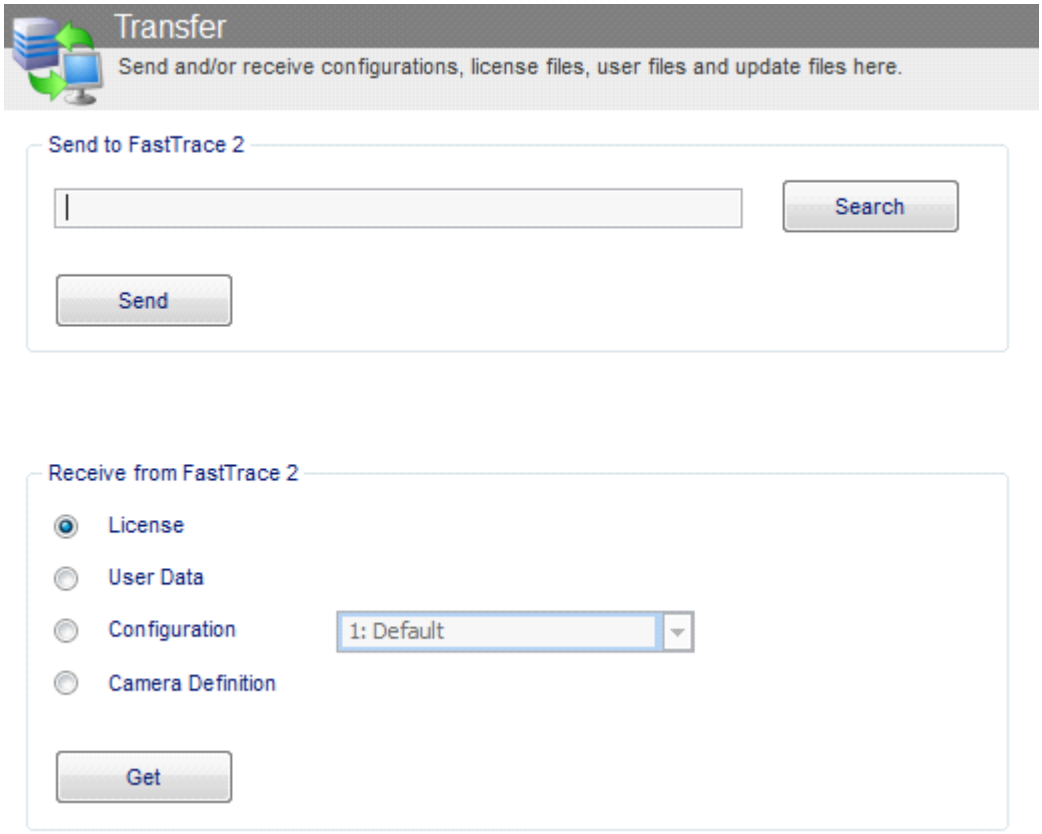
Click **Save** to apply the new settings.

17 Firmware, license, configuration

It is possible to upload and/or download several file types to and from the FastTrace 2 video system. The file type can be recognized from the file extension:

- .bin = software (linux + application)
- .lic = license
- .usr = user data
- .prop = configuration
- .def = camera definitions

Open **System > Maintenance > Transfer**.



(see FastTrace 2 User Manual for detailed information)

Mind:

You can download a license from a FastTrace 2 server on firmware version 2.5 (or lower version) and upload this license into a FastTrace 2 server on firmware version 2.6. Although the license formats have changed in the new firmware version 2.6, the “older” license will be automatically converted.

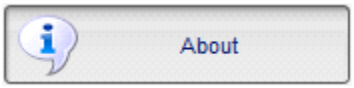
However, it is not possible to load a license file from a FastTrace 2 server on firmware version 2.6 into a FastTrace 2 server on firmware 2.5 (or lower).

17.1 License types

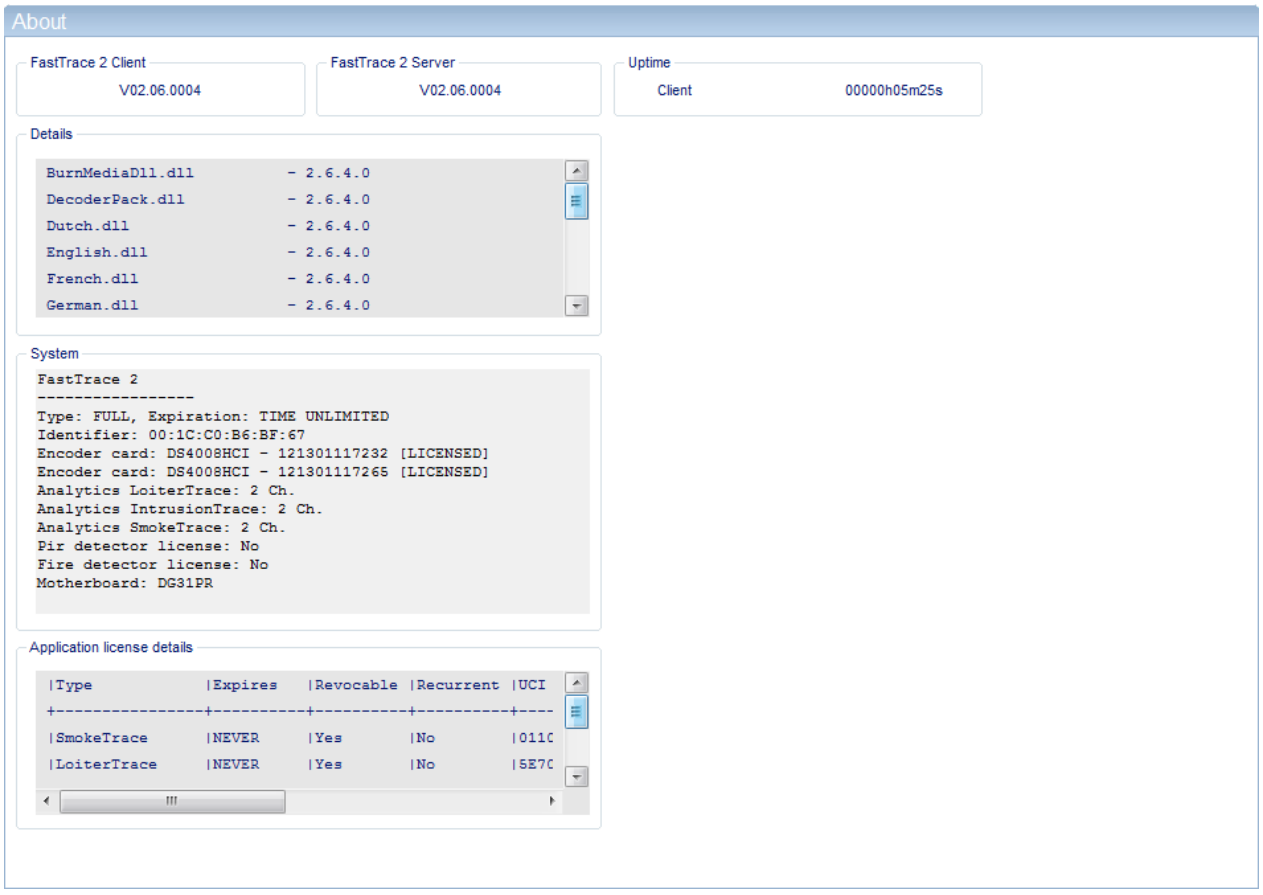
You can load different types of license in the video system:

- System license (*see* System license)
- Encoder license (= a license for the analogue video cards in the video system)
- Application license (= a license to be able to use an extra application)
  > IntrusionTrace (= video analytics application for video perimeter detection)
  > LoiterTrace (= video analytics application for video indoor loitering detection)
  > Fire-IO (= interface application enabling the alarm management and transmission of fire alarms from a fire panel)
  > PIR-HLI (= interface application enabling alarm reception, configuration and walk testing using the PRO detectors databus)

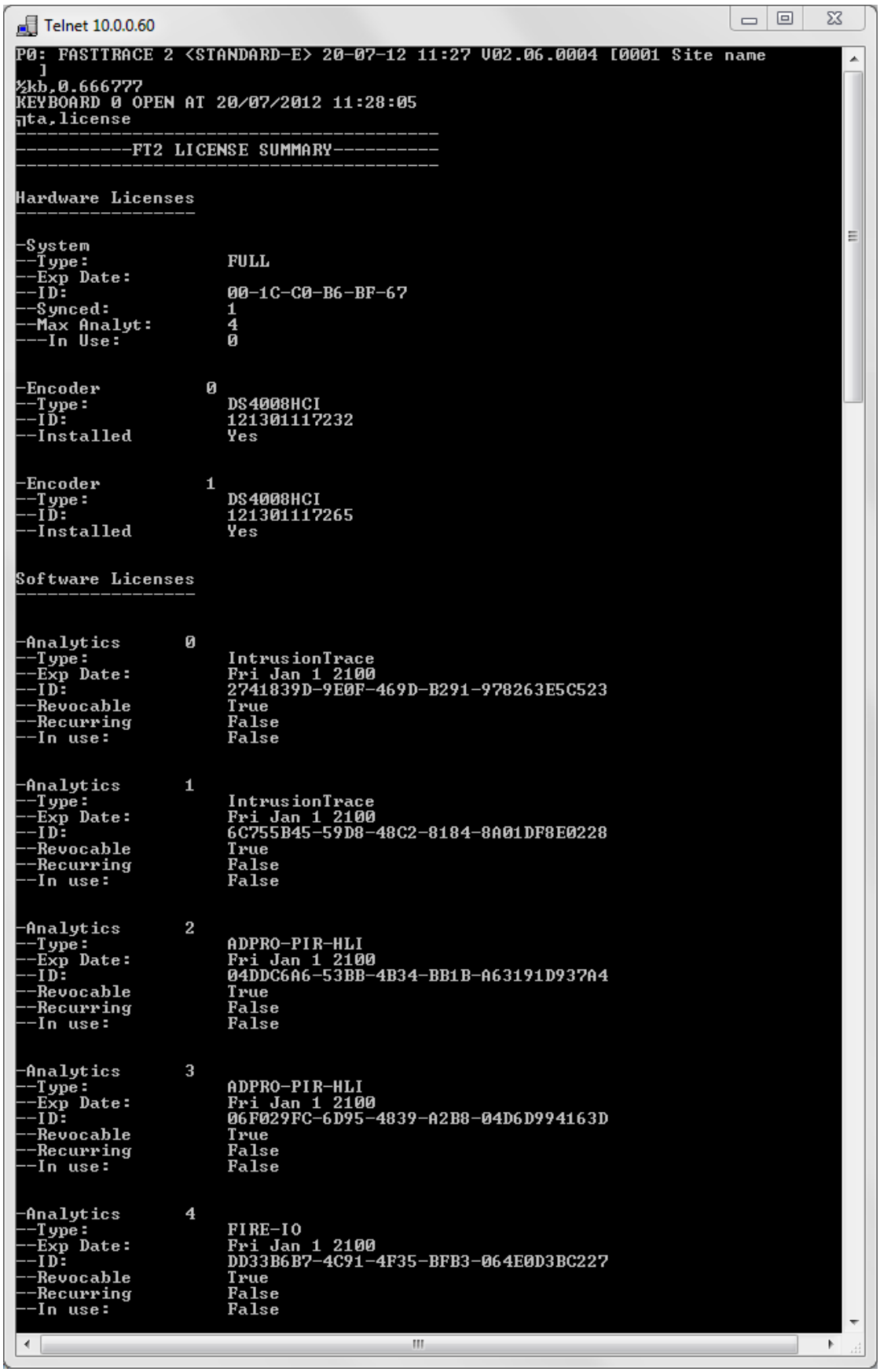
You can see what licenses have been loaded into your video system via the ‘About’ button.



The information about the licenses is shown in the *License* section:



If you don’t have the FastTrace 2 Client software, you can get the desired licenses information from a telnet connection, using the command “ta, license”.


Telnet 10.0.0.60
P0: FASTTRACE 2 <STANDARD-E> 20-07-12 11:27 V02.06.0004 [0001 Site name]
½kb,0.666777
KEYBOARD 0 OPEN AT 20/07/2012 11:28:05
┐ta,license
FT2 LICENSE SUMMARY
Hardware Licenses
-System
--Type: FULL
--Exp Date:
--ID: 00-1C-C0-B6-BF-67
--Synced: 1
--Max Analyt: 4
---In Use: 0
-Encoder 0
--Type: DS4008HCI
--ID: 121301117232
--Installed Yes
-Encoder 1
--Type: DS4008HCI
--ID: 121301117265
--Installed Yes
Software Licenses
-Analytics 0
--Type: IntrusionTrace
--Exp Date: Fri Jan 1 2100
--ID: 2741839D-9E0F-469D-B291-978263E5C523
--Revocable True
--Recurring False
--In use: False
-Analytics 1
--Type: IntrusionTrace
--Exp Date: Fri Jan 1 2100
--ID: 6C755B45-59D8-48C2-8184-8A01DF8E0228
--Revocable True
--Recurring False
--In use: False
-Analytics 2
--Type: ADPRO-PIR-HLI
--Exp Date: Fri Jan 1 2100
--ID: 04DDC6A6-53BB-4B34-BB1B-A63191D937A4
--Revocable True
--Recurring False
--In use: False
-Analytics 3
--Type: ADPRO-PIR-HLI
--Exp Date: Fri Jan 1 2100
--ID: 06F029FC-6D95-4839-A2B8-04D6D994163D
--Revocable True
--Recurring False
--In use: False
-Analytics 4
--Type: FIRE-IO
--Exp Date: Fri Jan 1 2100
--ID: DD33B6B7-4C91-4F35-BFB3-064E0D3BC227
--Revocable True
--Recurring False
--In use: False

17.2 System license

From version 02.00.0000 all ADPRO video systems require a system license. This applies of course also to the FastTrace 2 video system (version 02.01.0007).

Mind: the perimeter and loitering detection, and also the video (encoder) cards require a separate licence and are **not** included in the system licence!

There are 3 types of system license available:

- FULL: all features of the video system can be used;
- ENTRY(*): all features are available, with these restrictions:
  - only 4 analogue cameras can be used (no IP camera support);
  - only 1 hard disk can be used;
  - only 1 MIO card (and no EIO cards) is supported;
- TRANSMITTER: all features are available, but there is no continuous recording allowed and recording on event is fixed to 5 seconds on prerecording, 10 seconds on event recording and 0 seconds on postrecording.

(*) The ENTRY system license is not possible with the FastTrace 2☒ configuration!

A FastTrace 2 video system running without system license, will behave as a video system with FULL license for 5 days. The user will however, be informed of the license error via the event message LICENSE_SYSTEM_ERROR and by a popup window at each connection with the FastTrace 2 Client.

After that period of 5 days the video system will enter a “locked down” state and will refuse all connections for live streams and recordings. All active recordings will continue on the video system. During this locked down state, the FastTrace 2 Client shows only the “About” window (so that you can retrieve the necessary information to order a new license) and the “Transfer” window (so that you can upload a license to the FastTrace 2 video system).
(*see also the FastTrace 2 User Manual: uploading a license)*

Remarks:

The system license is locked on the FastTrace 2 motherboard and is therefore system specific: the correct MAC address should be included in the license.

When you upload the system license and your unit has already other licenses (e.g. encoder license, loitering license …), your video system will merge all these licenses together in one license file. That way you can download this one file for backup and archiving purposes.

17.3 Application license

The ADPRO FastTrace 2 and FastTrace 2☒ platforms – from version 2.6 onwards – provide the ability to unlock extra functionality which resides in its system firmware. This unlocking is achieved through the activation of an application license on the unit. Extra functionality can be added to the system by buying a FastTrace 2 Application Credit token through your regular channel. The Application Credit Token is a credit that can represent one or more application licenses of one or multiple types.

An application license contained within the Application Credit Token can have an unlimited or timed validity. A timed validity application license expires x time after it has been consumed for the first time. An unlimited application license will never expire. Yet, timed application licenses will stop operating at the moment they expire. The FastTrace 2 unit will signal this through the transmission of expiry events. It is the responsibility of the user/installer of the system to make sure that the application remains active, if desired of course, by installing a new and valid application license to replace the expired one.

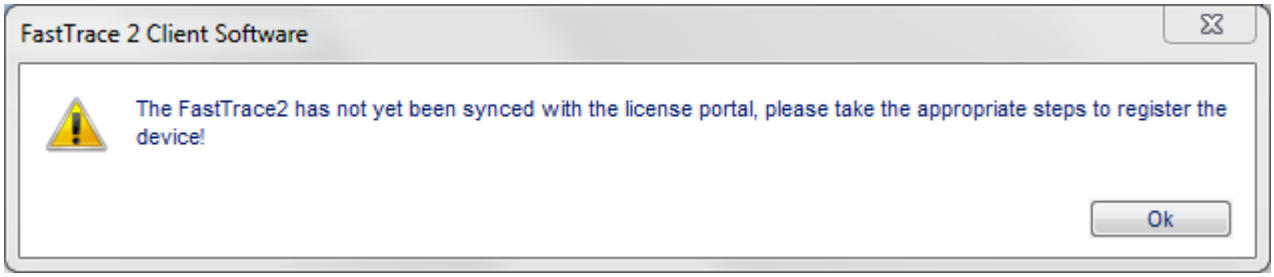
Once you have acquired a FastTrace 2 Application Credit Token you can consume this credit to your account. In order to be able to do this you will have to sign up for an account on the Xtralis Application License Web portal. Please see the *Application License Guide* for more information on this.

Whenever you enter the credit number, mentioned on the credit token, to your account you will find that all application licenses that are bound to this credit token will be added to your account. A credit token cannot be assigned a second time. Do mind: it is the responsibility of the owner of the credit token to handle it in a secure way to avoid wrong usage and loss of this asset. Lost credit tokens cannot be handled or replaced in any way by the manufacturer.

There are 4 types of applications that can be added to the FastTrace 2 or FastTrace 2☒ functionalities:

1. IntrusionTrace
2. LoiterTrace
3. Fire-IO
4. PIR-HLI

When upgrading to the FastTrace 2 software version 2.6 you will automatically convert your existing analytics licenses to the new license formats. This will result in the following warning:


FastTrace 2 Client Software
The FastTrace2 has not yet been synced with the license portal, please take the appropriate steps to register the device!
Ok

You will thus need to synchronize your FastTrace 2 unit with the licenses portal. Please read the *Application License Guide* for further information!

17.3.1 IntrusionTrace

The IntrusionTrace is a video analytics application for video outdoor perimeter detection applications.

See FastTraceTM 2 IntrusionTrace.

17.3.2 LoiterTrace

The LoiterTrace is a video analytics application for video indoor loitering detection applications.

See FastTraceTM 2 LoiterTrace.

17.3.3 Fire-IO

The Fire-IO is an interface application enabling the alarm management and transmission of fire alarms from a fire panel.

See Alarm profiles.

This license will be available at a later time!

17.3.4 PIR-HLI

The PIR-HLI is an interface application enabling alarm reception, configuration and walk testing using the PRO detectors databus.

17.4 Checking the software version

At regular times new firmware and software updates are released. These new releases can be downloaded from the website http://www.xtralissecurity.com.

To check what version of the FastTrace 2 (server and client) you can use the client software.

Click ‘About’.

You will get the information about the FastTrace 2 Client version and the FastTrace 2 Server version:

It is always recommended to have both Client and Server on the same version, but in principle different versions can be used.

17.4.1 Upgrade the Client version to the Server version

If the Client version is a lower version that the Server version, you will get a popup window when connecting to the Server with the Client:

FastTrace 2 Client Software
There is a new version of the FastTrace 2 client software available for download. You can upgrade your client software by deinstalling the current software and connecting again to the FastTrace 2 server using a webbrowser!
[Current version 02.01.0006 - available version 02.01.0007]
Ok

The Client version is always included in the firmware of the video system.

Remove the current Client software from you PC via **Start > All Programs > FastTrace 2 > Uninstall**. Then connect to the FastTrace 2 Server with the internet browser to reinstall the client software.

17.4.2 Downloading the new client software version from the Xtralis Support website.

Surf to http://www.xtralissecurity.com and log in.

If you do not have any login details, please sign up via this website.

17.5 Installation of the FastTrace 2 firmware

17.5.1 Installation requirements

To execute a FastTrace 2 version 2.01.0007 installation you need:
- Windows PC
- FastTrace 2 image (= file with extension ".img")
- FastTrace 2 Image Flash application (version 1.0.3 or higher)
- FastTrace 2 USB stick (with at least 512 MB writing space)
- Monitor/screen
- Keyboard

Mind:

The FastTrace 2 Server is by default equipped with a DANE-ELEC USB stick. In principle the video system can use any kind of USB stick, but it cannot be guaranteed other types of USB stick will work faultless. The type Kingston DataTraveler, for example, regularly proves to be unreliable.

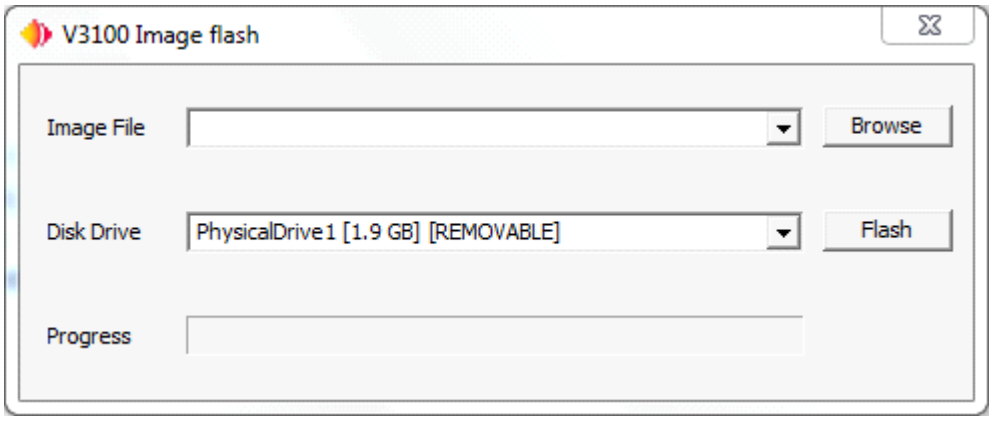
For a detailed list of supported USB sticks, please consult our website http://www.xtralissecurity.com.

When your video system has an **Intel DH55TC** motherboard, your video system is equipped with an **SSD disk**. In that case you will need a *hard disk interface SATA* for SSD disks (to connect to your PC via USB).

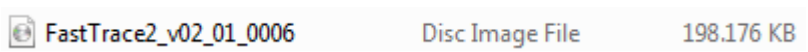
17.5.2 Installation procedure

Remove the boot USB stick / SSD disk from the FastTrace 2 video system and connect it to your Windows PC. Copy the image file and the Image Flash application on the PC.

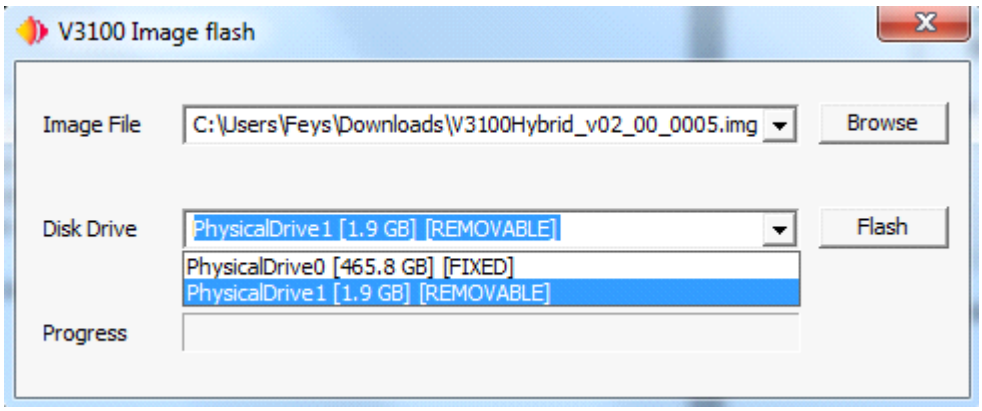
Start the application Image Flash on the Windows PC:



Select for "Image File" the image file: FastTrace2_v02_xx_xxxx.img.



Select the USB stick / SSD disk for Disk Drive.



Click ‘Flash’.

When you have flashed the USB stick / SSD disk, remove it from your Windows PC and connect it to your FastTrace 2 video system. Also connect monitor/screen and keyboard to the video system.

Start the video system and wait for the boot window. Then take these steps:
- Select FastTrace 2 Installer and choose “Update Current System”;
- Select “Format (all) recording disk(s)” (this may take some time!);
- Select “Main menu” and choose “Reboot”.

The video system will now reboot with the factory settings. The IP adres is by default 10.0.0.10.

The video system will work on FULL license for 5 days. It is recommended to upload your license to the FastTrace 2 Server within this period.
(*see FastTrace 2 Users’ Manual)*

17.6 Upgrade the FastTrace 2 firmware

Before upgrading, it is recommended to back up your license, configuration(s), user data and camera definitions!
(*see* *Downloading files from the video system*)

Important:

You can upgrade your video system firmware if you have already at least version 1.02 installed on the FastTrace 2 Server (FastTrace, V3100 FT, V3100 HYBRID version 1). If not, you cannot upgrade and you need to do a new installation. (*see* Installation of the FastTrace 2 firmware)

Please read the FastTrace 2 Field Alert #1 for more information on upgrading V3100 systems!

17.6.1 Upgrade requirements

You can upgrade the firmware from the FastTrace 2 Client software using the BIN file. When you cannot use the client software, you will need to flash the img file to the FastTrace 2 Server.

To upgrade your FastTrace 2 Server to version 2.01.0051 by flashing the img file, you need:
- Windows PC
- FastTrace 2 image (= file with extension ".img")
- FastTrace 2 Image Flash application (version 1.0.3 or higher)
- FastTrace 2 USB stick (with at least 512 MB writing space)
- Monitor/screen
- Keyboard

Mind:

The FastTrace 2 Server is by default equipped with a DANE-ELEC USB stick. In principle the video system can use any kind of USB stick, but it cannot be guaranteed other types of USB stick will work faultless. The type Kingston DataTraveler, for example, regularly proves to be unreliable.

When your video system has an **Intel DH55TC or DH61BE** motherboard, your video system is equipped with an **SSD disk**. In that case you will need a *hard disk interface SATA* for SSD disks (to connect to your PC via USB).

17.6.2 Downloading a new firmware version from the Xtralis Support website.

Surf to http://www.xtralissecurity.com and login.

If you do not have login details, please register on this site.

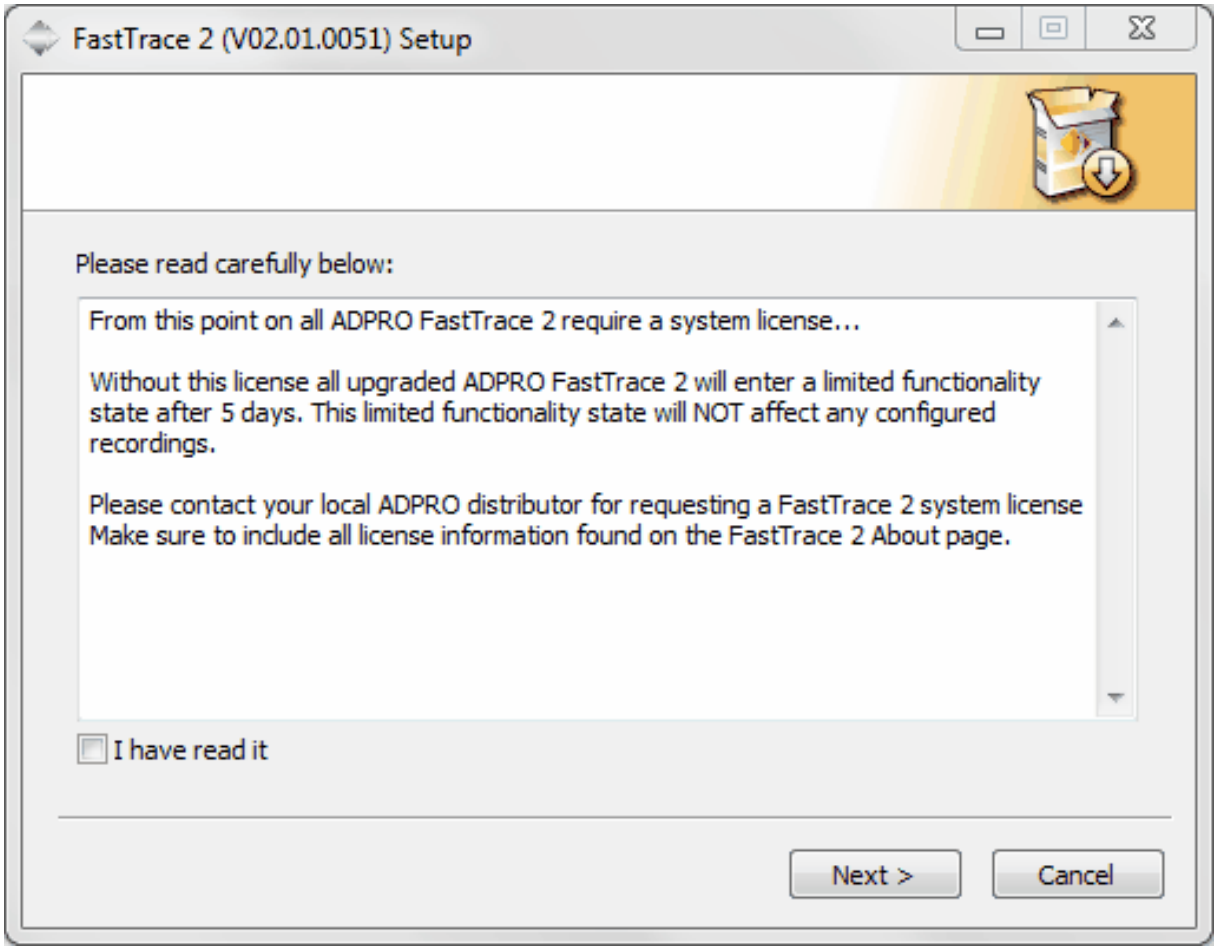
17.6.3 Upgrade procedure

There are 2 possible procedures:

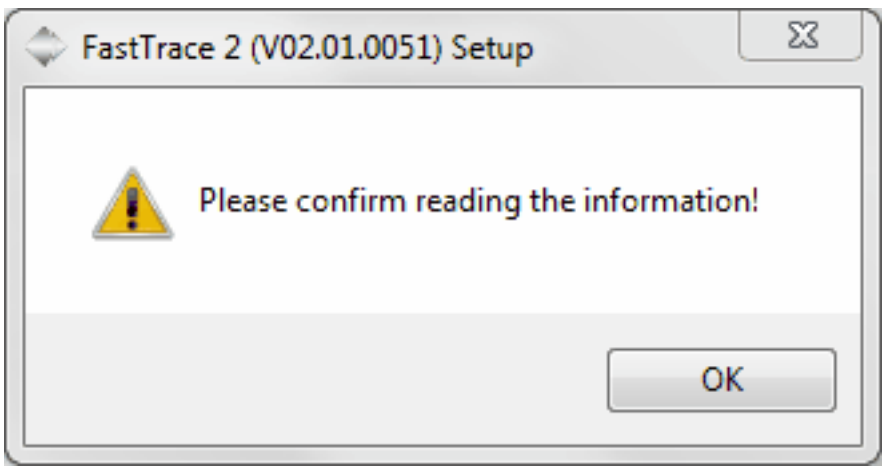
- using a BIN file
- using an IMG file

17.6.3.1 Upgrade firmware with BIN file

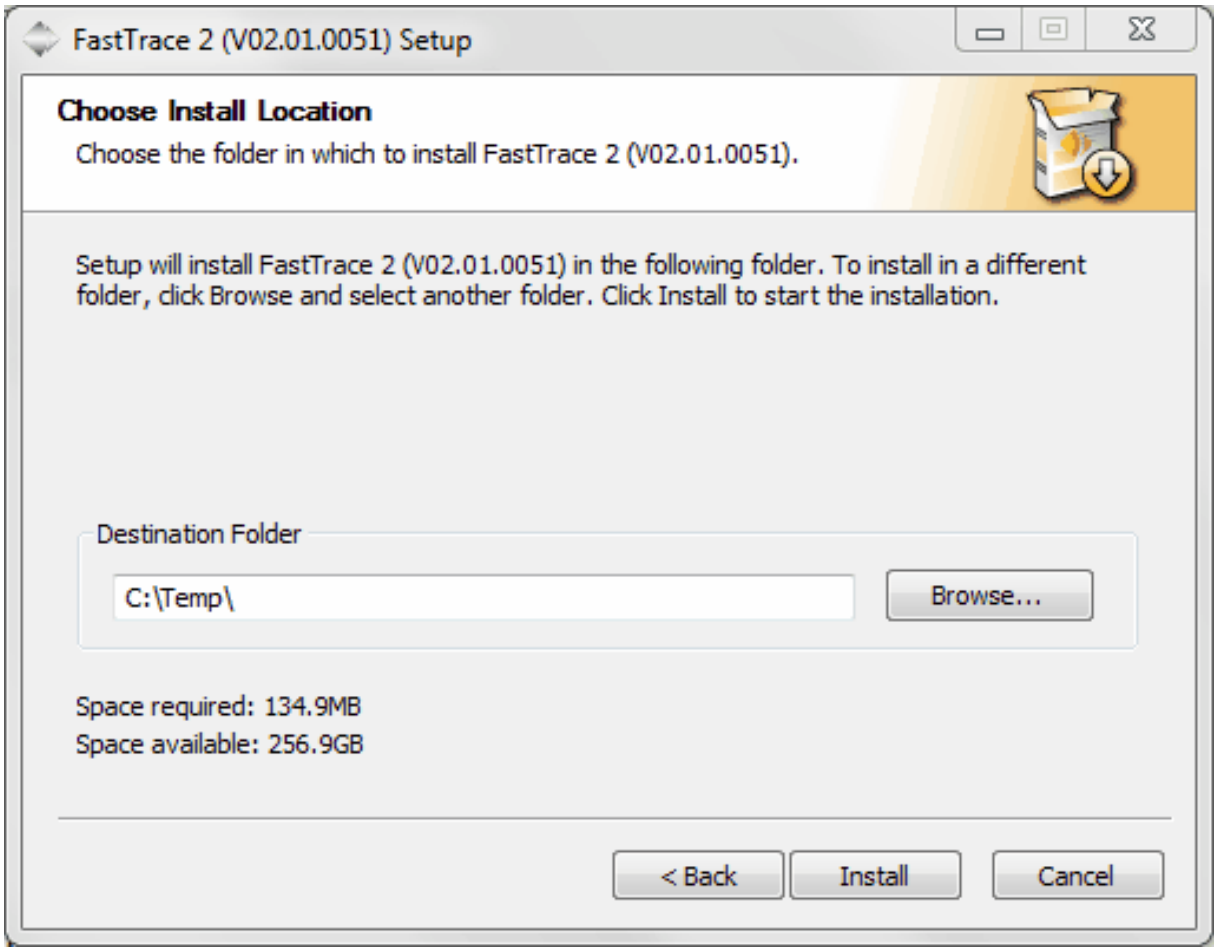
Download the firmware upgrade from the Xtralis Security website. Launch this application:


FastTrace 2 (V02.01.0051) Setup
Please read carefully below:
From this point on all ADPRO FastTrace 2 require a system license...
Without this license all upgraded ADPRO FastTrace 2 will enter a limited functionality state after 5 days. This limited functionality state will NOT affect any configured recordings.
Please contact your local ADPRO distributor for requesting a FastTrace 2 system license Make sure to include all license information found on the FastTrace 2 About page.
I have read it
Next >
Cancel

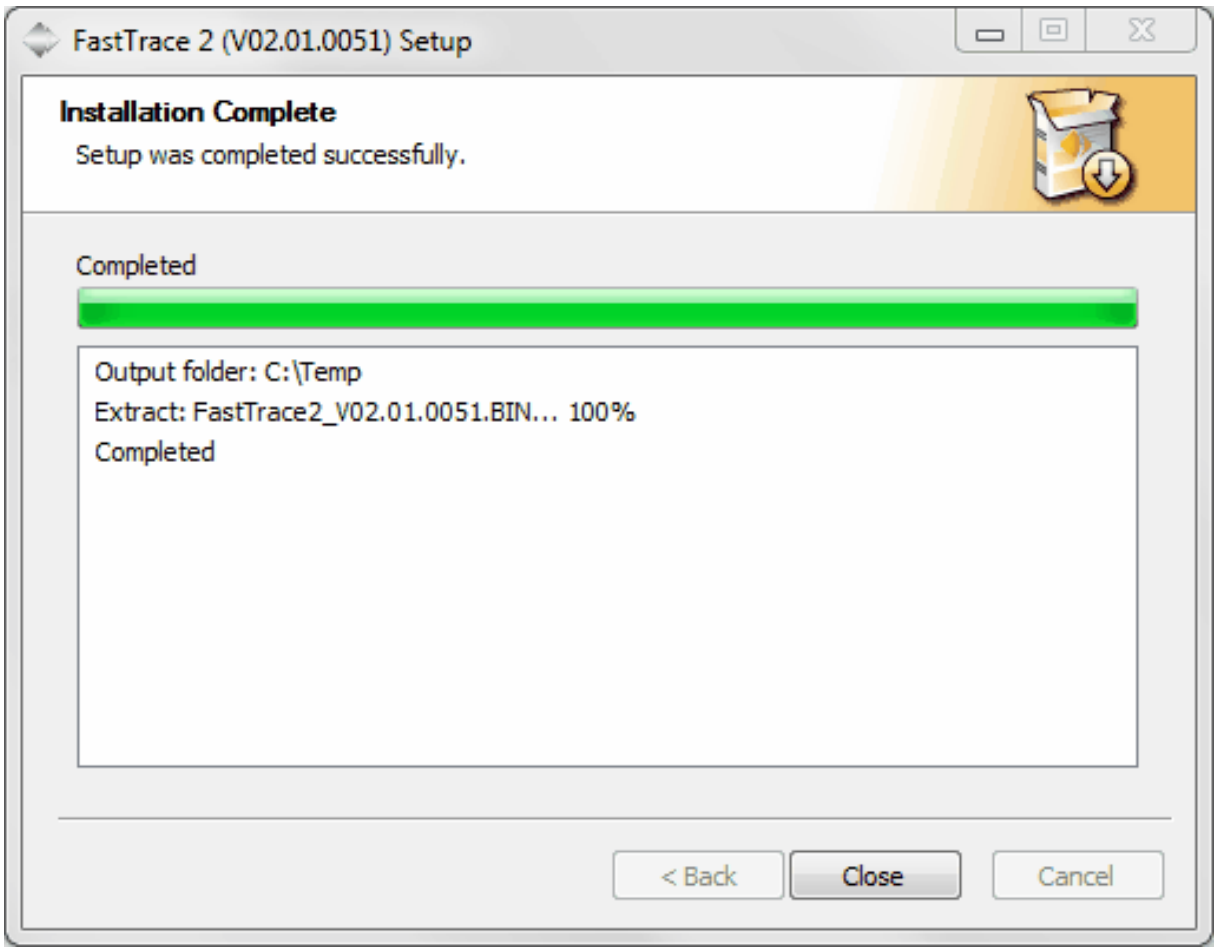
Do not forget to tick *I have read it*, or you will receive the following error message when clicking **Next**:



Click **Next**.


FastTrace 2 (V02.01.0051) Setup
Choose Install Location
Choose the folder in which to install FastTrace 2 (V02.01.0051).
Setup will install FastTrace 2 (V02.01.0051) in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Temp\
Browse...
Space required: 134.9MB
Space available: 256.9GB
< Back
Install
Cancel

Click **Browse** to change the destination folder. Click **Install** to extract the BIN file to the folder you have selected.

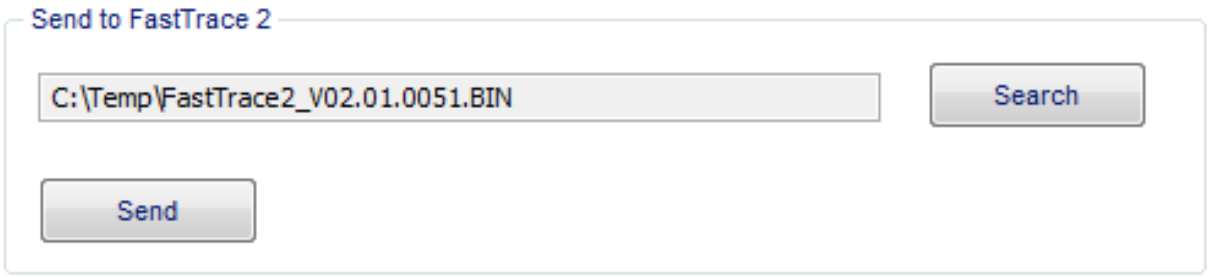


Click **Show details** to see the information on the installation.

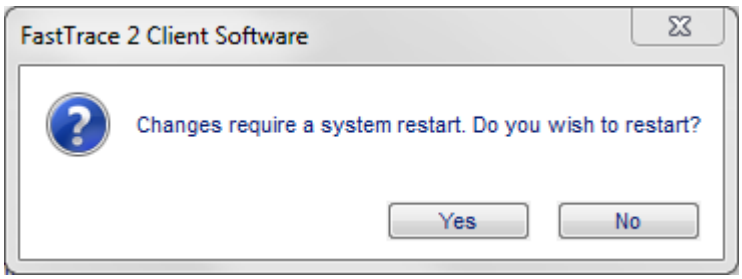
Click **Close**.

Next, open the folder in which you have installed the BIN file to check whether the BIN file has been extracted correctly.

To upgrade the firmware, open the FastTrace 2 Client software, open **System > Maintenance > Transfer** and upload (via the **Search** button) the BIN file.



Click **Send** to upgrade. You will need to reboot your video system.

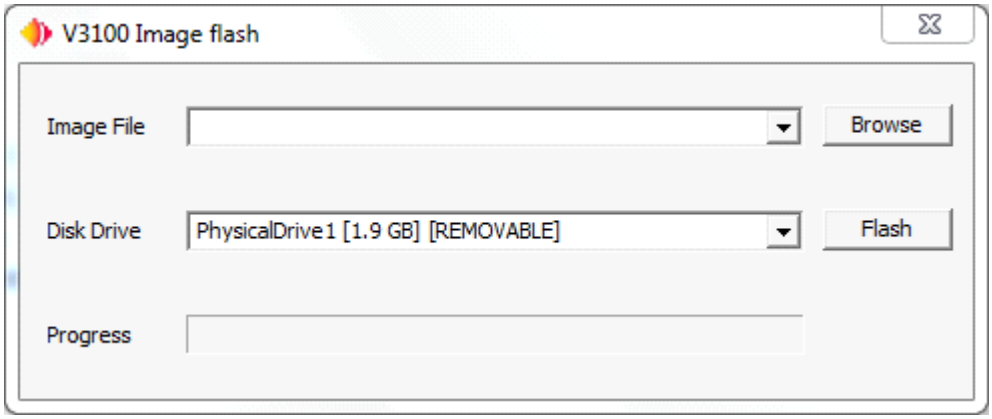


17.6.3.2 Upgrade firmware with img file

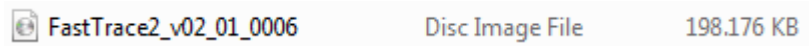
Remove the boot USB stick / SSD disk from the FastTrace 2 video system and connect it to your Windows PC. Copy the image file and the Image Flash application on the PC.

If you cannot see the drive for the SSD disk, you need to create a partition in Windows. Open Control Panel > Administrative Tools > Computer Management > Disk Management > Create new partition. Select FAT32 and choose a letter for the drive.

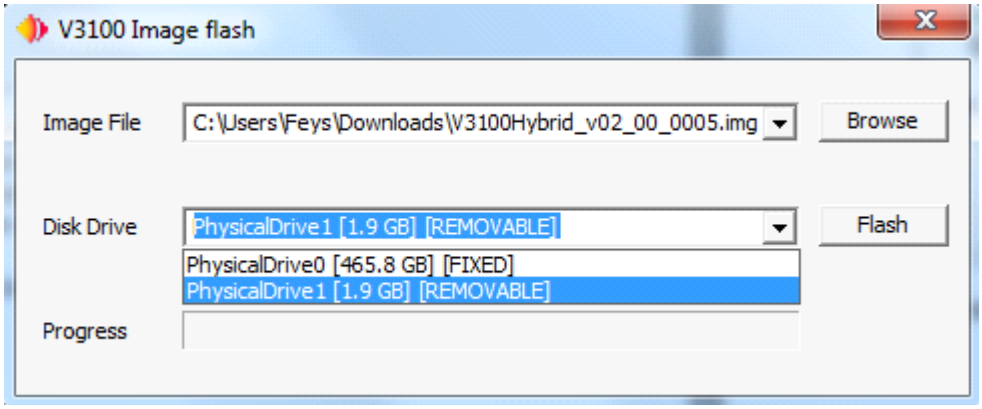
Start the application Image Flash on the Windows PC:



Select for *Image File* the new image file: FastTrace2_v02_xx_xxxx.img.



Select the USB stick / SSD disk for *Disk Drive*.



Click **Flash**.

When you have flashed the USB stick / SSD disk, remove it from your Windows PC and connect it to your FastTrace 2 video system. Also connect monitor/screen and keyboard to the video system.

Start the video system and wait for the boot window. Then take these steps:
- Select FastTrace 2 Installer and choose “Update Current System”;
- Select “Format (all) recording disk(s)” (this may take some time!);
- Select “Main menu” and choose “Reboot”.

The video system will now reboot with the factory settings. The IP address is by default 10.0.0.10.
The video system will work on FULL license for 5 days. It is recommended to upload your license to the FastTrace 2 Server within this period.
(*see* *Uploading files to the video system*)

17.6.4 IP camera definitions

When upgrading the FastTrace 2 firmware, the custom ipcam.def file will be removed. After the upgrade the FastTrace 2 video system will use the native ipcam.def file.

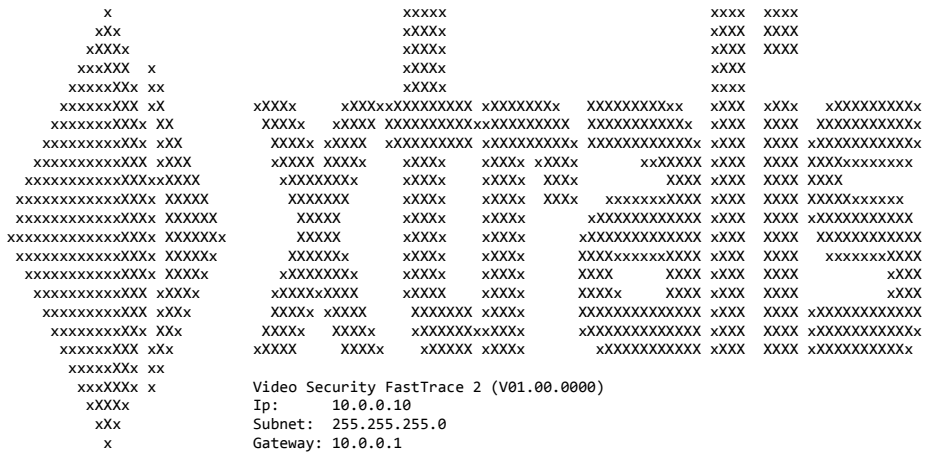
18 Additional information

18.1 Retrieving the IP address of the FastTrace 2

Connect a monitor/screen to the FastTrace 2 video system. If the video matrix is active, you can close the matrix by pressing the key combination <Ctrl> <Alt> <F1>.

Reboot the video system (either from the FastTrace 2 Client or by pressing the key combination <Ctrl> <Alt> <Delete>.

The video system will need some time to restart. The current IP address will be shown on the welcome window:



18.2 Diagnostics

In case of major troubles with the FastTrace 2 video system, the system allows to generate a lot of traces. In some cases, after having contacted the Xtralis Support Division, you will be asked to activate and capture some traces and files that can be helpful to resolve the trouble.

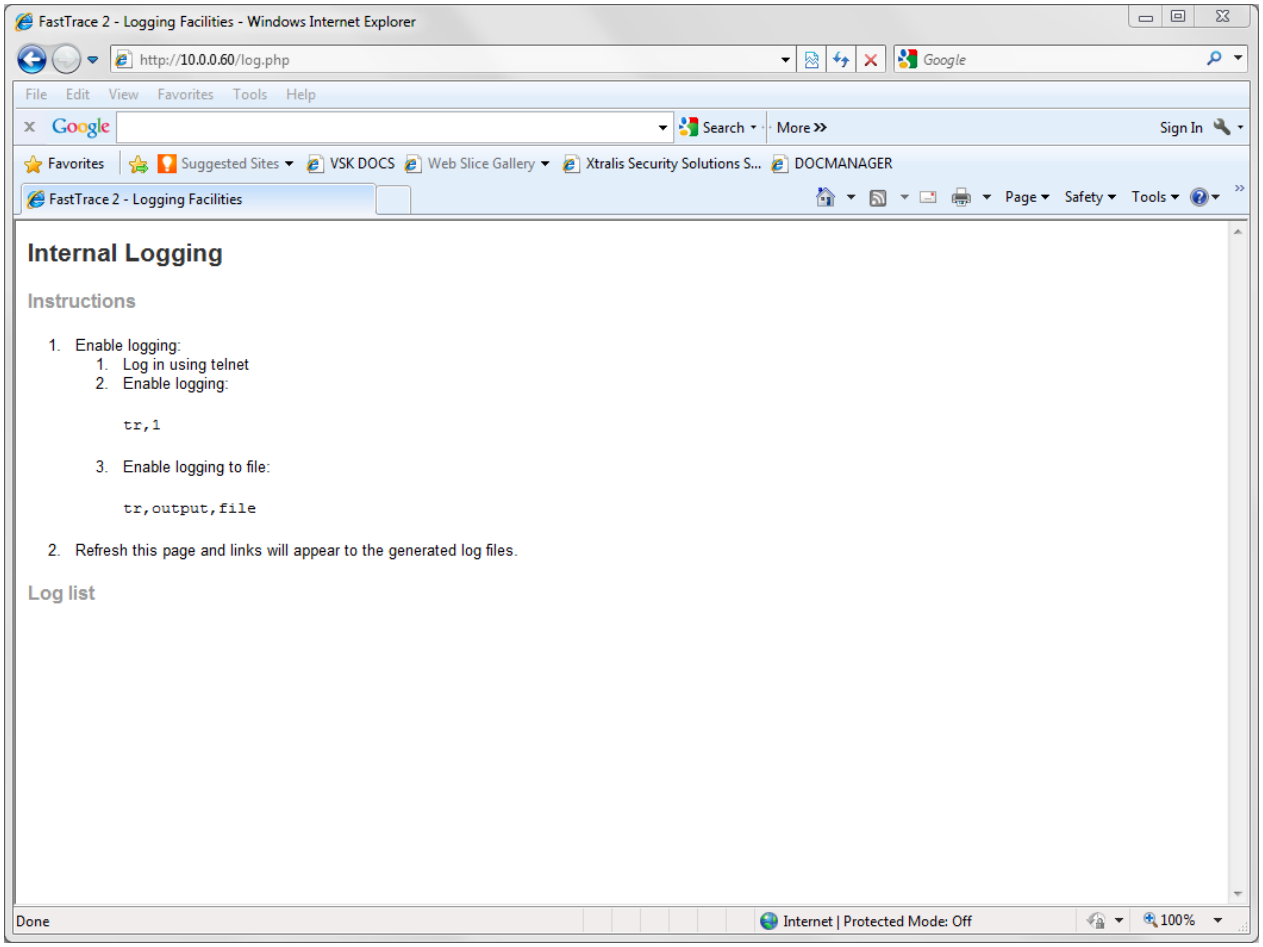
18.2.1 Retrieve traces

The FastTrace 2 can output its internal trace buffer to hard disk to allow tracing for longer periods of time without losing the data. This happens with the telnet command “tr,output,file”. To easily retrieve these files, enter the video system’s IP address in the address bar of your internet browser adding **/log.php** to the address.

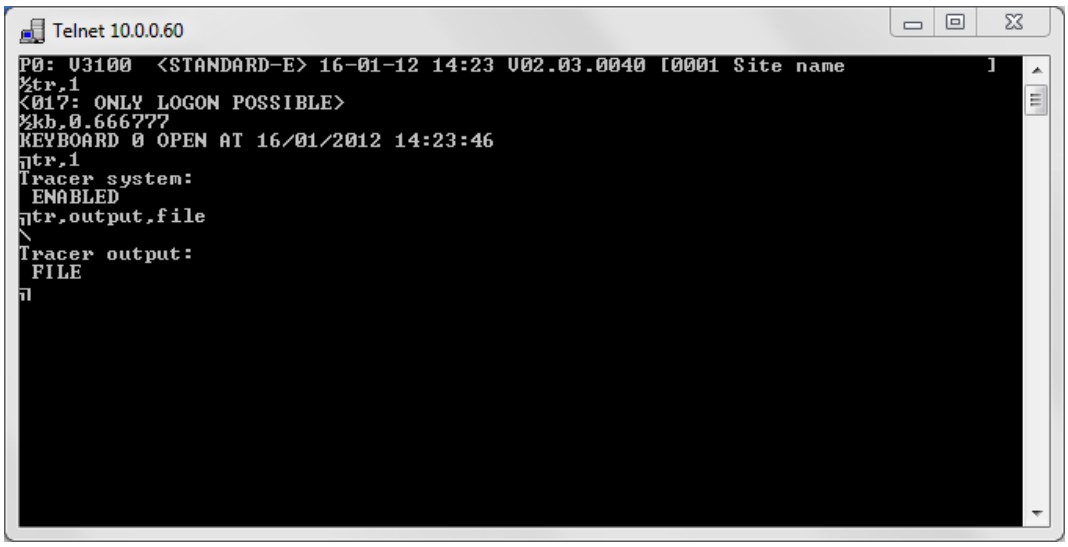
Example: http://10.0.0.10/log.php.

Here you can download the generated log files.

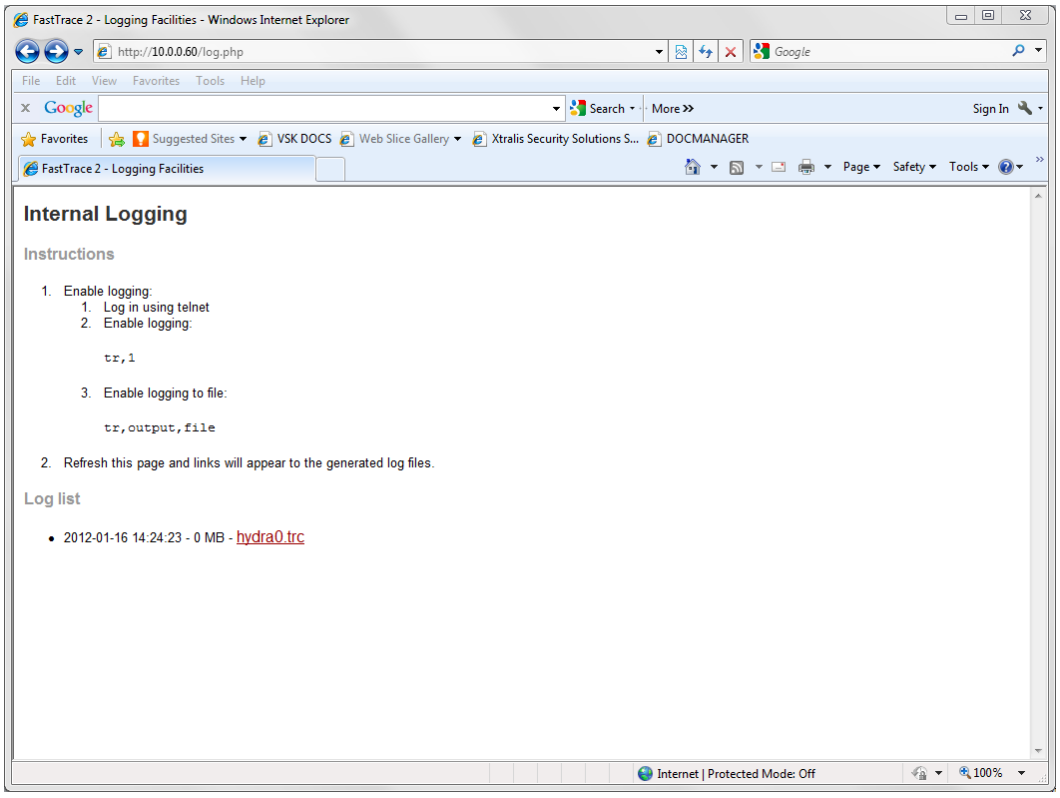
When you open the web page without having enabled logging, you will get the Internal Logging page with the instructions you need to execute before you can actually receive the log files.



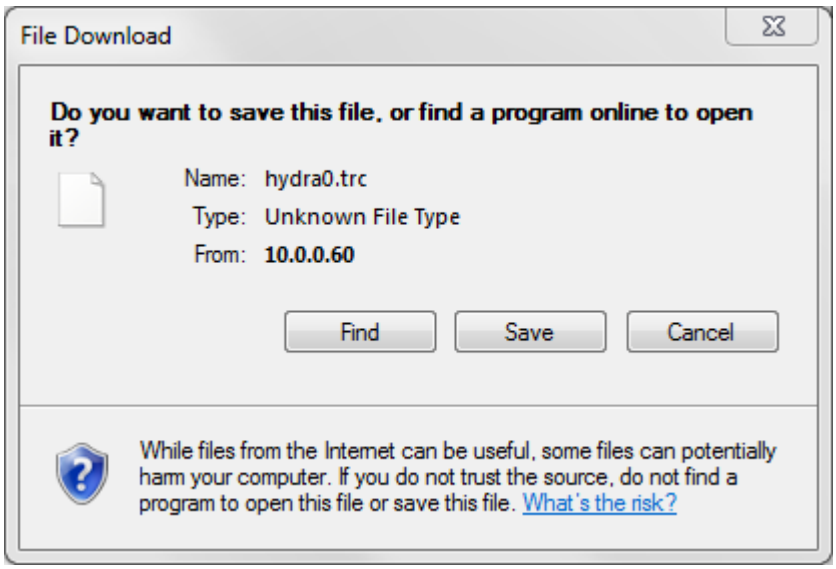
You need to enable the logging possibility before you can create a logging.



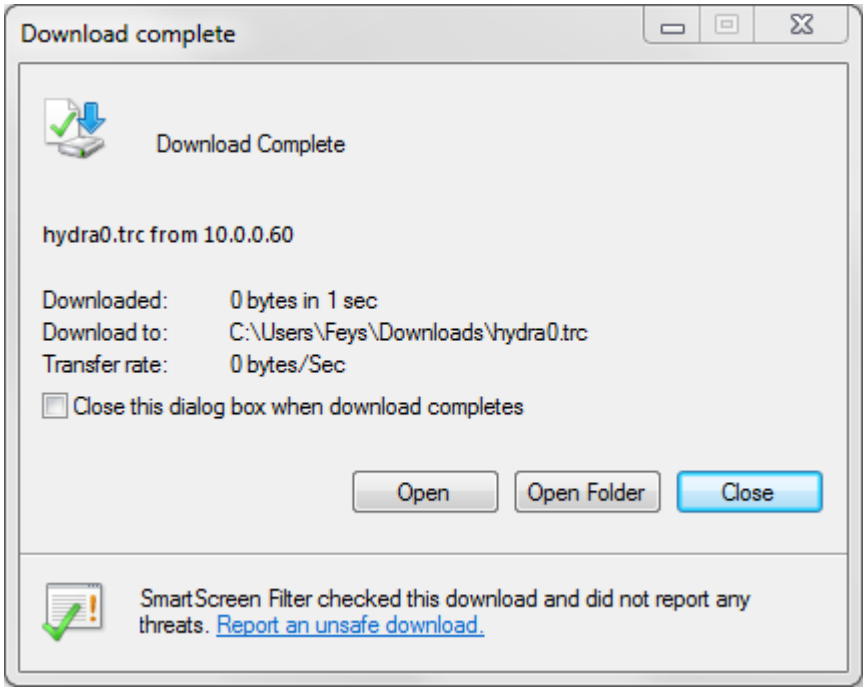
Click the link on the web page.

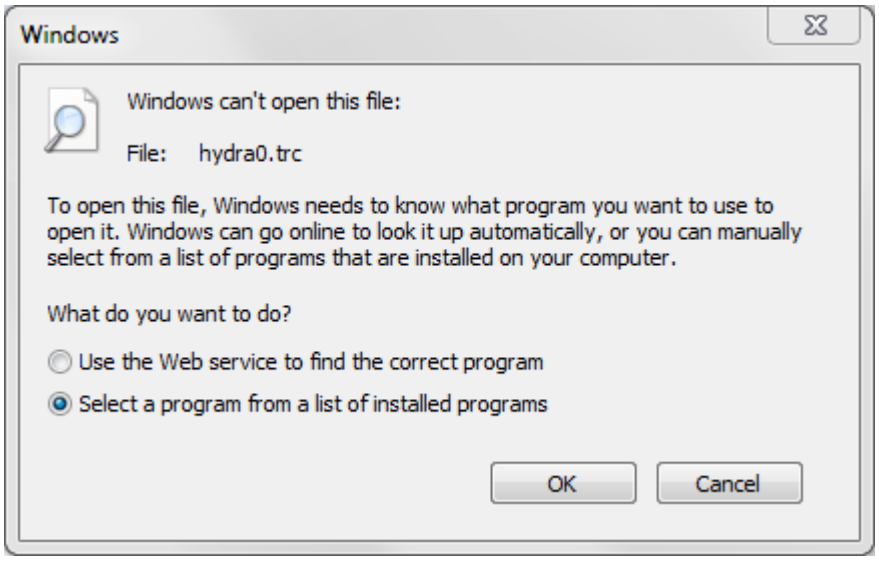

FastTrace 2 - Logging Facilities - Windows Internet Explorer
http://10.0.0.60/log.php
Internal Logging
Instructions
1. Enable logging:
1. Log in using telnet
2. Enable logging:
tr,1
3. Enable logging to file:
tr,output,file
2. Refresh this page and links will appear to the generated log files.
Log list
2012-01-16 14:24:23 - 0 MB - hydra0.trc

Next click **Save** to store the file on your PC or a network folder. Do not try to find a program online, because this will provide unexpected websites.


File Download
Do you want to save this file, or find a program online to open it?
Name: hydra0.trc
Type: Unknown File Type
From: 10.0.0.60
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Click Open and choose Notepad as default application.

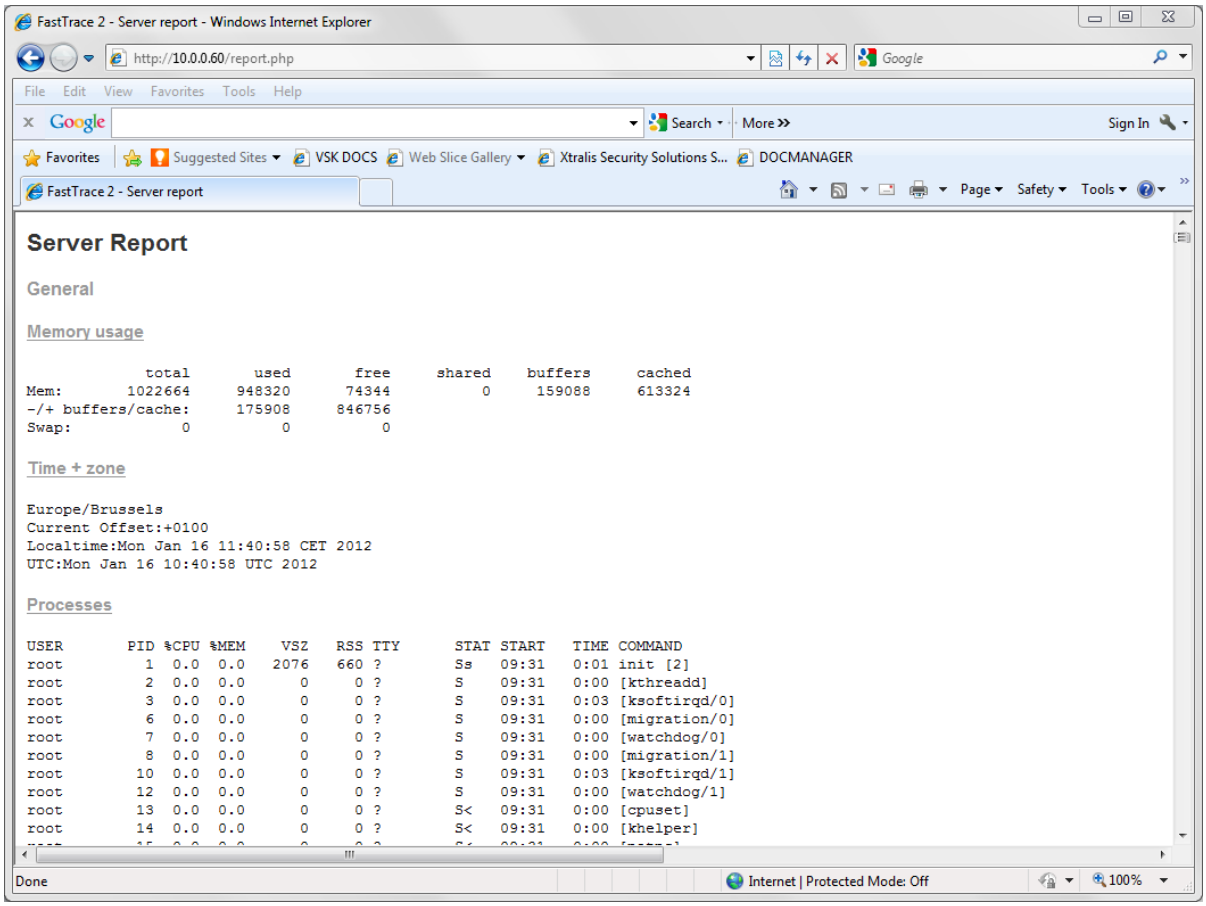

Download complete
Download Complete
hydra0.trc from 10.0.0.60
Downloaded: 0 bytes in 1 sec
Download to: C:\Users\Feys\Downloads\hydra0.trc
Transfer rate: 0 bytes/Sec
Close this dialog box when download completes
Open
Open Folder
Close
SmartScreen Filter checked this download and did not report any threats. Report an unsafe download.


Windows
Windows can't open this file:
File: hydra0.trc
To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.
What do you want to do?
Use the Web service to find the correct program
Select a program from a list of installed programs
OK
Cancel

18.2.2 Retrieve reports

The FastTrace 2 video system also generates reports. You can view these reports via the internet browser. Enter the IP address of the video system in the address bar of the browser adding **/report.php** to the IP address.

Example: http://10.0.0.10/report.php.


FastTrace 2 - Server report - Windows Internet Explorer
http://10.0.0.60/report.php
FastTrace 2 - Server report
Server Report
General
Memory usage
total used free shared buffers cached
Mem: 1022664 948320 74344 0 159088 613324
-/+ buffers/cache: 175908 846756
Swap: 0 0 0
Time + zone
Europe/Brussels
Current Offset:+0100
Localtime:Mon Jan 16 11:40:58 CET 2012
UTC:Mon Jan 16 10:40:58 UTC 2012
Processes
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 2076 660 ? Ss 09:31 0:01 init [2]
root 2 0.0 0.0 0 0 ? S 09:31 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 09:31 0:03 [ksoftirqd/0]
root 6 0.0 0.0 0 0 ? S 09:31 0:00 [migration/0]
root 7 0.0 0.0 0 0 ? S 09:31 0:00 [watchdog/0]
root 8 0.0 0.0 0 0 ? S 09:31 0:00 [migration/1]
root 10 0.0 0.0 0 0 ? S 09:31 0:03 [ksoftirqd/1]
root 12 0.0 0.0 0 0 ? S 09:31 0:00 [watchdog/1]
root 13 0.0 0.0 0 0 ? S< 09:31 0:00 [cpuset]
root 14 0.0 0.0 0 0 ? S< 09:31 0:00 [khelper]
Done
Internet | Protected Mode: Off
100%

These items are shown on the Server Report:

General	Memory usage
	Time + zone
	Processes
	Uptime
Performance	Vmstat
	IO stat
	PID stat
	MP stat
Network	Interfaces – available
	Interfaces – enabled
	Routes
	Listen ports
	Netstat – all
	DEV stats
	Sockstat
	ARP cache

Filesystem	Mounts
	S.M.A.R.T
	Fsck
	Open files
	Free disk space
Hardware	CPU
	Memory
	Mainboard
	PCI
	Udev database
Server	Server version
	Server process memory usage
	Files
	Active config

Contact the Xtralis Support Division for further assistance.

18.2.3 VSKWin: retrieve the FastTrace 2 configuration file

The FastTrace 2 sends events to the VSKwin software.
To set up the FastTrace 2 for alarm transmission:

- connect to the V3100 using the V3100 client;
- open **System** > **Behaviour** > **Alarm transmission;**
- Select the **Primary Ethernet** option;
- For **FastTrace 2 Unit ID**, specify a unique identification number (0001 to 9999);
- For **Destination 1 IP address**, enter the IP address of the VSKwin computer;
- Click **Save;**
- Open **System** > **Maintenance** > **Configuration,** select your active configuration and click **Save**.

All FastTrace 2 events can be assigned to instructions or can be associated to an alarm indicator on a map.
To retrieve the list of inputs from a FastTrace 2 video system:

- Connect to the V3100 system with the FastTrace 2 client.
- Open **System** > **Maintenance** > **Transfer** menu.
- Select the **Configuration** option, choose your active configuration and click the **Get** button.
- The file FastTrace2_xxxx_0.prop will be stored on your computer (xxxx is the identification number of the connected FastTrace 2 system). Use the search function in Windows to find this file.
- Copy this file to your data folder and rename it to propxxxx.cfg.

18.2.4 VSKWin: Create an alarm text that automatically opens a live camera image

Create a new text file under C:\Program Files\VSK Electronics\data\DETINT\Cxxxx where xxxx represents the ID number of the FastTrace 2 video system. Rename the file to Dyyyy+.HTM where yyyy represents the number of the event (example 1034 corresponds to motion detection in zone 1 on camera 1). Edit this file with Notepad, and type the following lines (the example opens camera 1 on the video system that is on IP address 10.0.2.45):

```
<html>
<body>
<iframe
src="http://10.0.2.45/index.php?autostartmask=1&username=0&password=666777&nogui"
width=100% height=100%>
</body>
</html>
```

18.2.5 Activate timer output on FastTrace 2

Purpose: execute a macro in VSKWin that activates an output on the FastTrace 2 for x seconds.
Requires: an unused NetIO or USBIO input, eg I2595.
We will use C2576 as timer output.

Step 1 Create a macro in VSKWin:
Click **Tools** > **Macro Editor**
Type the following lines: IP,+,2595
IP,-,2595
Save under \data\macro\FastTrace2\active timer output.cmd

Step 2 Program input 2595 for a hold time of 30 seconds:
In VSKWin, click **Modules** > **System manager**
Open **Video panels**
Right click your V3100 video system and click **Web config**
In the Web configurator, open **System** > **Behaviour** > **Input/output behaviour**
Select event **I 2595**
Enter a description, select *Silent message* to suppress alarm messages, and set the alarm hold time to 30 seconds
Click **Save**

Step 3 In the FastTrace 2 system, program an output that follows the state of the chosen input
In the Web configurator, open **System** > **Behaviour** > **Input/output behaviour**
Select output **C2576**
Enter a description, tick the option **Logic**, and double click on the input I2595
Click **Save**

Step 4 In VSKWin, open **Modules**, **Command centre**.
Tick the video system in the left window pane and open the **Macro** tab.
Select your macro and click the **Execute** button !

Mind:

From version 2.5 onwards you can add a hold time for each output. See Alarm inputs.

18.3 Error codes

18.3.1 General error codes

Code	ERROR	Description
0	NO_ERROR	
-10	ERROR_INVALID_VIDEO_CHANNEL	Invalid video channel.
-11	ERROR_INVALID_VIDEO_RESOLUTION	Invalid video resolution.
-12	ERROR_INVALID_VIDEO_QUALITY	Invalid video quality.
-13	ERROR_INVALID_VIDEO_BITRATE	Invalid bitrate.
-14	ERROR_INVALID_VIDEO_FRAMERATE	Invalid framerate.
-16	ERROR_INVALID_IPADDRESS	Invalid IP address.
-17	ERROR_INVALID_PORTNUMBER	Invalid port number.
-18	ERROR_INVALID_USER	Invalid user ID.
-19	ERROR_INVALID_USER_PASSWORD	Invalid user password.
-20	ERROR_INVALID_INSTANCE	Invalid instance.
-21	ERROR_INVALID_DECODER_NUMBER	Invalid decoder number.
-22	ERROR_INVALID_VOLUME	Invalid audio volume.
-23	ERROR_INVALID_OPERATION_MODE	Invalid operation mode.
-24	ERROR_NO_CONTROL_CONNECTION	No control protocol connection established yet.
-25	ERROR_INVALID_BITRANGE	Invalid bitrange.
-26	ERROR_BUFFER_TOO_SMALL	Supplied buffer too small.
-27	ERROR_IN_USE	Already in use.
-28	ERROR_NOT_IN_USE	Not in use.
-29	ERROR_SEARCH_INVALID_CAMMASK	Invalid camera mask.
-30	ERROR_SEARCH_INVALID_TIME	Invalid search time.
-31	ERROR_SEARCH_INVALID_CONDITIONS	Invalid search criteria.
-32	ERROR_SEARCH_FAILED	The search function failed.
-33	ERROR_INVALID_PAGE	An invalid system page was specified.
-34	ERROR_INVALID_PARAM	An invalid parameter was supplied.
-35	ERROR_GETTING_USERRIGHTS	Error getting the users rights.
-36	ERROR_INSUFFICIENT_USERRIGHTS	The user hasn't got sufficient rights to execute this command.
-37	ERROR_AUDIOTX_INUSE	
-38	ERROR_AUDIOTX_NOT_INUSE	
-39	ERROR_GETAUDIO_PARAMS	
-41	ERROR_GETTING_CAMTYPE	
-42	ERROR_GETTING_RESOLUTIONS	
-43	ERROR_NOT_AVAILABLE	
-44	ERROR_GET_FASTTRACE2_FIRMWAREVERSION	
-45	ERROR_GET_3PICS_DISTANCE	
-46	ERROR_GET_AUDIO_CFG	
-47	ERROR_NO_TIMESTAMP_FOUND	
-48	ERROR_PICTURE_TAMPERED	
-49	ERROR_NO_RESULTS	

18.3.2 Control protocol error codes

These error codes represent errors connecting to the client protocol server. The error codes can be both negative or positive. Positive error codes represent Microsoft socket errors (errors returned by the WSAGetLastError() function call, see Microsoft documentation for an explanation of these error codes).

Code	ERROR	Description
-50	ERROR_CONNECT_RESOLVE_IP	Connect function failed in gethostbyname() function call.
-51	ERROR_CONNECT_FAILED	Connection to the client protocol server failed.
-52	ERROR_CONNECT_START_LISTEN	Failed to start the control protocol listen thread.
-53	ERROR_CONNECT_SEND_MESSAGE	Failed to send a message to the control protocol server.
-54	ERROR_CONNECT_INVALID_REPLY	Unexpected reply while connecting to the control protocol server.
-55	ERROR_CONNECT_USER_PASSWORD	Invalid username - password combination.
-56	ERROR_SEND_FAILED	Failed to send a command to the control protocol server.
-57	ERROR_SEND_NO_REPLY	No reply received from the control protocol server within the specified timeout.
-58	ERROR_INVALID_PARAMS	Invalid parameters.
-59	ERROR_INVALID_REPLY	Invalid reply to a command.
-60	ERROR_COMMAND_FAILED	The command was not executed properly.
-61	ERROR_MAX_CONNECT_REACHED	Maximum number of connections reached.
-62	ERROR_OPEN_FILE	Error opening file (send & get file command).
-63	ERROR_FILE_OPERATION	Error performing a file operation.
-64	ERROR_CONNECT_NOTECHACCESS	Error connecting due to no technician grant.
-65	ERROR_COULD_NOT_ARM_DISARM	Error (dis)arming the system.
-66	ERROR_CANNOT_SWITCH_VM22A	Error switching the VM22A.
-67	ERROR_UNKNOWN_COMMAND_SEND	
-68	ERROR_CONNECT_USER_BLOCKED	
-69	ERROR_PICS_EMPTY	
-70	ERROR_PICS_INCOMPLETE	
-71	ERROR_PICS_NOVIDEO	
-72	ERROR_CONNECTED_BUTNOREPLY	
-73	ERROR_KEY_VALUE	
-74	ERROR_CMS_ACTIVE	

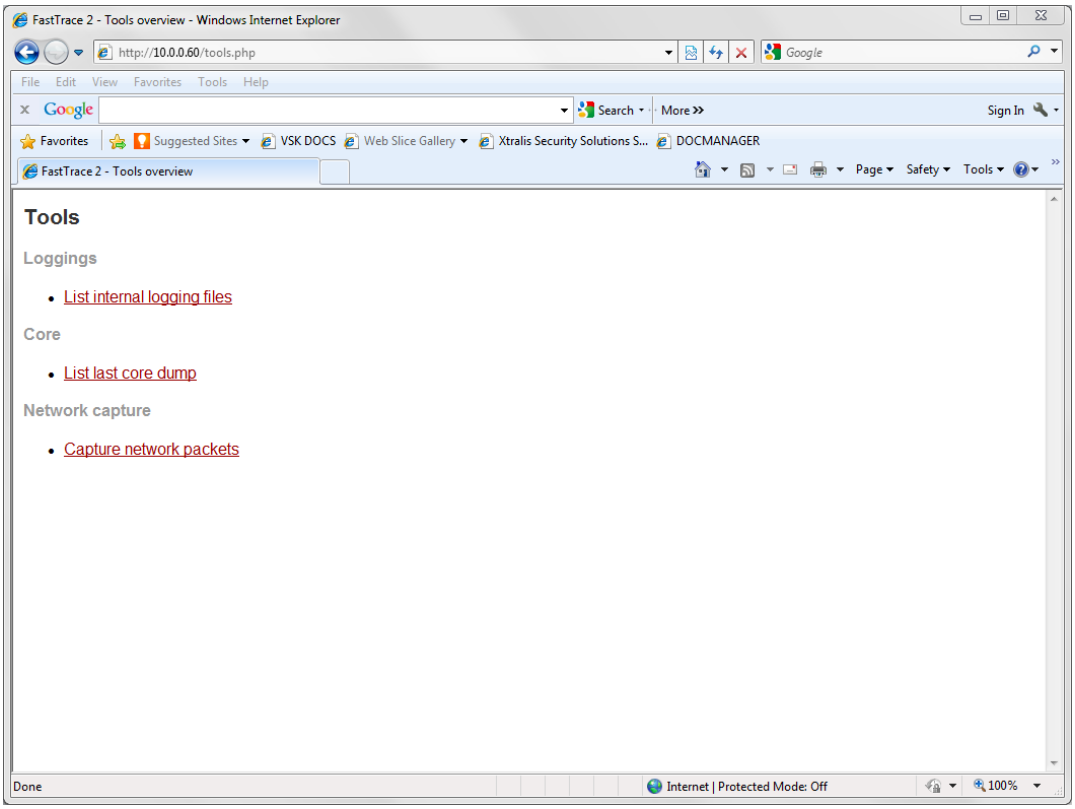
18.3.3 Filter graph/codec error codes

Code	ERROR	Description
-100	ERROR_DLL_VERSION	Decoder DLL version not high enough.
-110	ERROR_NO_DDRAW_SUPPORT	Graphical card error.
-120	ERROR_NO_BLIT_SUPPORT	Graphical card error.
-130	ERROR_FILTER_GRAPH	Error starting / stopping / pauzing the filter graph.
-140	ERROR_START_SINK	Error starting the sink filter.
-150	ERROR_START_YUV_TRANSFORM	Error starting the YUV transform.
-155	ERROR_START_DECODER_TRANSFORM	Error starting the decoder filter.
-160	ERROR_START_SOURCE	Error starting the source filter.
-170	ERROR_STOP_SOURCE	Error stopping the source filter.
-180	ERROR_NO_SOURCE	Error no source filter.
-190	HIK_ERROR_PORT	Invalid decoder instance.
-200	HIK_ERROR_INVALID_PARAM	Invalid parameters.
-210	HIK_ERROR_INVALID_STATE	Can't perform this action in this state.
-220	HIK_ERROR_OPEN_FILE	Error opening file.
-230	HIC_ERROR_CLOSE_FILE	Error closing file.
-240	HIK_ERROR_ZERO_FILE_LEN	Empty file.
-250	HIK_ERROR_START_PLAY	Error starting video playback.
-260	HIK_ERROR_STOP_PLAY	Error stopping video playback.
-270	HIK_ERROR_PAUZE_PLAY	Error pauzing video playback.
-280	HIK_ERROR_CONTINUE_PLAY	Error continuing video playback.
-285	HIK_ERROR_NO_DATA	Error no data.
-290	HIK_ERROR_START_AUDIO	Error starting audio playback.
-300	HIK_ERROR_STOP_AUDIO	Error stopping audio playback.
-310	HIK_ERROR_SET_AUDIOVOLUME	Error setting audio volume.
-320	HIK_ERROR_SET_FRAME	Error setting playback frame.
-330	HIK_ERROR_GET_VIDEOSIZE	Error getting the video source width and height.
-350	HIK_ERROR_GENERATE_DATA	Error generating data.
-360	HIK_ERROR_GET_SAMPLE	Error getting sample.
-370	HIK_ERROR_DISPLAY_CALLBACK	Error installing the decoder callback
-400	HIK_ERROR_HEADER	Invalid video header.
-410	HIK_ERROR_REC_START	Error starting recording.
-420	HIK_ERROR_REC_STOP	Error stopping recording.
-430	HIK_ERROR_REC_OPEN	Error opening recording.
-440	HIK_ERROR_REC_WRITE	Error writing recording.
-450	HIK_ERROR_FILE_EXISTS	File already exists.
-460	HIK_ERROR_SET_OPERATIONMODE	Error setting operation mode.
-470	HIK_ERROR_SET_THROW_BFRAME	Error instructing the decoder to drop decoding of certain B frames.
-480	HIK_ERROR_USERDATA_CALLBACK	Error installing the user data callback.
-490	HIK_ERROR_NOTHING_RECORDED	Nothing was recorded.
-500	HIK_ERROR_ALLOC	Null pointer passed.
-510	HIK_ERROR_SET_RESOLUTION_CHANGEMSG	
-520	HIK_ERROR_SET_FILEEND_MSG	
-530	HIK_ERROR_SET_WATERMARK_CALLBACK	Failed to install watermark callback.
-550	HIK_ERROR_SETSTREAMOPENMODE	Error setting stream mode.
-560	HIK_ERROR_OPENSTREAM	Error opening stream.
-570	HIK_ERROR_CLOSESTREAM	Error closing stream.
-580	HIK_ERROR_READHEADER	Error reading video header.
-590	HIK_ERROR_CLEAR_BUF	Error clearing decoder buffers.
-600	HIK_ERROR_STOP_DECODING	Error stopping the decoding.
-610	HIK_ERROR_RENDERER_SLOW	
-650	ERROR_MISSING_H264_AAC_DECODER	

-660	ERROR_MISSING_H264_DECODER	
-670	ERROR_MISSING_AAC_DECODER	
-700	ERROR_INVALID_PARAMS	Invalid parameters.
-710	ERROR_INVALID_USERID	Invalid user ID.
-720	ERROR_INVALID_IPADDR	Invalid IP address.
-730	ERROR_SET_RTPOVERRTSP	Error setting TCP streaming.
-740	ERROR_SET_MULTICAST	Error setting multicast streaming.
-750	ERROR_INVALID_CHANNEL	Invalid video channel.
-760	ERROR_MAX_RENDERERS	Max renderers.
-770	ERROR_UNKNOWN_RENDERER	Unknown renderer.
-780	ERROR_WRONG_EXTENSION	Wrong file extension.
-800	LIVE_ERROR_CREATE_TASKSCHEDULER	Error creating RTSP task scheduler.
-810	LIVE_ERROR_CREATE_BASICUSERENV	Error creating RTSP usage environment.
-820	LIVE_ERROR_CREATE_RTSPCLIENT	Error creating RTSP client.
-830	LIVE_ERROR_DESCRIBE_URL	Error sending RTSP describe command.
-840	LIVE_ERROR_CREATE_MEDIASESSION	Error creating media session.
-850	LIVE_ERROR_PLAY_MEDIASESSION	Error playing media session.
-860	LIVE_ERROR_INVALID_SESSION	Invalid media session.
-870	LIVE_ERROR_FORCE_STOP	Had to kill the netsource thread.
-880	LIVE_ERROR_THREAD_START	Error starting receive thread.
-890	LIVE_ERROR_NO_VIDEO_CODEC_FOUND	No suitable video codec found.
-900	LIVE_ERROR_NO_AUDIO_CODEC_FOUND	No suitable audio codec found.
-910	LIVE_ERROR_INVALID_SDP_LINE	Invalid session description protocol line.
-920	LIVE_ERROR_GET_CONFIG	Invalid config returned by server.
-950	ERROR_FILEMAP_CREATE	Failed to create the interprocess communication.
-960	ERROR_NAMEDEVENT_CREATE	Failed to create the interprocess communication.
-970	ERROR_CREATE_PROCESS	Failed to start the communication process.
-980	ERROR_NO_REPLY_FROM_PROCESS	No reply from the communication process.
-990	ERROR_RTSP_CONNECT_FAILED	RTSP connection failed.
-1000	CODEC_ERROR_NOT_FOUND	Codec not found.
-1010	ERROR_TOO_MANY_FRAMES_IN_QUEUE	
-1020	ERROR_CONNECTION_LOST	

18.4 FastTrace 2 web pages

There are several web pages to consult with the FastTrace 2. To open these web pages in your internet browser you need to type the IP address in the addres bar, followed by the extensions as described in the table underneath.

Web page	Description
index.php	This is the main page of the FastTrace 2. When the FastTrace 2 has been installed, this page automatically opens the FastTrace 2 Client application (see Launching the FastTrace 2 client in Internet Explorer). When the application has not yet been installed, you will be redirected to the setup page (setup.php).
setup.php	On this page you can download the client application (see Installing the FastTrace 2 Client Software).
tools.php	This page contains the links to the internal logging, the core dump and the network trace: 
log.php	Here you can download the log files (see Retrieve traces).
report.php	Here you can consult essential information on the configuration (see).
core.php	Here you can download the core dump (crash info) and watch dump (hang info) when you encounter these specific problems. You might be asked by our Support Division to send these files to them for further investigation. Please always mention the version when providing a core dump!
phpshell.php	This is a linux console through a web browser. You need a login and password to use this tool. This is by default only accessible for the Xtralis Development Team.
net.php	Here you will find a network sniffer for network tracing. This might come inhandy to check why a certain client cannot connect to the FastTrace 2 server.

19 Labelling of products

All ADPRO products are labelled.

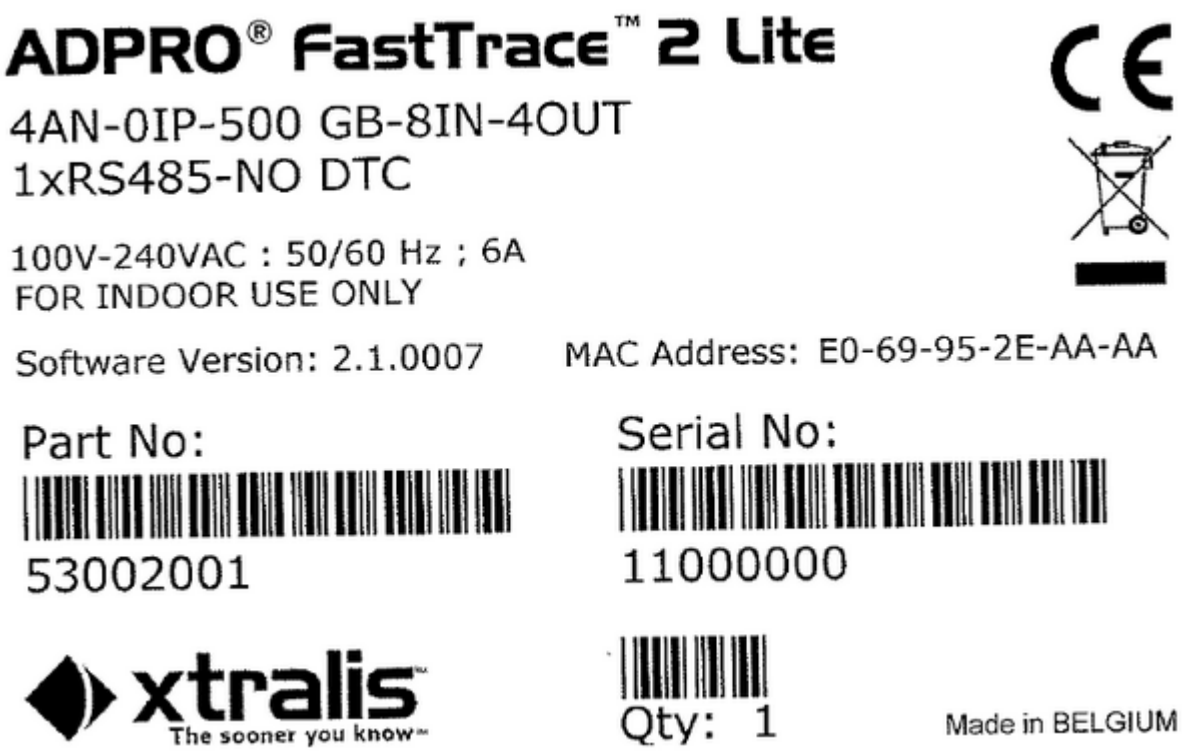
Older systems:

DEVICE	MARKING ON DEVICE	MARKING ON PACKING
FastTrace 2	XTRALIS Security Solutions BELGIUM TYPE : ADPRO FastTrace 2 ASSY number 54VHHID0 - YYMM 100-240VAC ; 50/60Hz ; 6A FOR INDOOR USE ONLY sn. YYYY – 54VHHID0- nnnn	XTRALIS Security Solutions BELGIUM TYPE : ADPRO FastTrace 2 ASSY number 54VHHID0 - YYMM 100-240VAC ; 50/60Hz ; 6A FOR INDOOR USE ONLY sn. YYYY – 54VHHID0- nnnn

Explanation :

54VHHID0 = version dependent, *see 0 Product number* structure
YY = year (2 digit)
MM = month
YYYY = year (4 digit)
nnnn = sequential number

Newest systems:



19.1 Product number structure

Each product version has an 8 digit product number, reflecting on the installed options.

The product number layout is made up as: 55 V HH I D 0

55	The FastTrace 2 Product Number
V	The video channel type: - 0 = 4 analogue - 1 = 8 analogue - 2 = 12 analogue - 3 = 16 analogue - 4 = 8 IP - 5 = 16 IP - 6 = 4 analogue and 8 IP - 7 = 8 analogue and 8 IP
HH	The hard disk size: - 00 = TX only (500 GB) - 01 = 500 GB - 02 = 1 TB - 03 = 2 TB - 04 = 3 TB - 05 = 4 TB - 06 = 5 TB - 07 = 6 TB - 08 = 7 TB - 09 = 8 TB - 10 = 9 TB - ...
I	I/O option: - 0 = no I/O - 1 = 1 MIO - 2 = 1 MIO + 1 EIO - 3 = 2 MIO - 4 = 2 MIO + 1 EIO - 5 = 2 MIO + 2 EIO
D	Down The Coax (DTC) option: - 0 = no DTC - 1 = DTC
0	Free digit

Example:

The product number 55602200 stands for:

- 4 analogue and 8 IP cameras
- 1 TB HDD
- 1 MIO + 1 EIO
- no DTC

19.2 Declaration of Conformity

Date :2011-09-13

ADPRO FastTrace2 EMC Test plan *Issue: 1.4*

Annex 7: Suppliers Declaration of Conformity (conform ISO17050)

1. Number of SDoC: SDoC_53/55VHHID0
2. Issuer's name: VSK Electronics NV, Venetiëlaan 39, 8530 Harelbeke, Belgium
3. Object of declaration: ADPRO FastTrace2
4. The object of declaration described above is in conformity with the requirements of the following documents:

   2004/108/EC EU EMC Directive (December 2004)
   EU Harmonised standard EN 61000-6-3 Generic emission standard – Residential and light industry
   EU Harmonised standard EN 50130-4: 1996 incl. A1 and A2, Alarm systems. Electromagnetic compatibility. Product family standard: Immunity requirements for components of fire, intruder and social alarm systems

   Radiocommunications Act 1992 of Australia, Radiocommunications labelling EMC notice 2008: CISPR 22:2005, class A

   FCC 47 CFR 15.109, radio frequency devices, sub part A unintentional radiators.

   A EMC Test Plan ref. EMC_ 53/55VHHID0 is available

5. Signed for and on behalf of: VSK Electronics NV
6. Date: 4 October 2011

Author, Name : Emmanuel Seynaeve Signature :	Verified, Name : Ivan Hendrikx Signature :	Approved, R&D Mgr. : Gerdy Maclbrancke Signature :

www.xtralis.com

The Americas +1 781 740 2223 **Asia** +852 2916 8894 **Australia and New Zealand** +61 3 9936 7000
Continental Europe +32 56 241 951 **UK** +44 1442 242 330 **and the Middle East** +962 6 5691083

The contents of this document are provided on an “as is” basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.
This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label.
This document is subject to copyright owned by Xtralis AG (“Xtralis”). You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify or publish any contents of this document without the express prior written consent of Xtralis.

ADPRO® by xtralis™